Zertifizierungsbericht

BS2000-SC Version 10.0

Gliederung des Zertifizierungsberichtes

1. Beschreibung des evaluierten Systems 3
1.1 System-Konfiguration..... 3
1.2 Liste der zum evaluierten System gehörigen Anwenderdokumentation.....23

2. Sicherheitsanforderungen.....24
2.0 Systemüberblick über die Grundversion BS2000 V10.0 24
2.1 Sicherheitsphilosophie 24
2.2 Sicherheitsfunktionalitäten.....40

3. Beschreibung der Evaluation mit Hinweisen auf kritische Bereiche.....53
3.1 Qualität der Sicherheitsanforderungen 53
3.2 Qualität der Spezifikation 54
3.3 Qualität der verwendeten Mechanismen.....54
3.4 Qualität der Abgrenzung zu nicht zu evaluierenden Systemteilen.....59
3.5 Qualität des Herstellungsvorgangs.....61
3.6 Betriebsqualität 62
3.7 Qualität der anwenderbezogenen Dokumentation.....63

4. Hinweise und Auflagen.....63

1. Beschreibung des evaluierten Systems

1.1 System-Konfiguration

BS2000 ist das Betriebssystem der Siemens-Nixdorf-Systemfamilie 7500, in der Rechner gängiger "Mainframe"-Architekturen - /370- und /370-XA-verwandte Architekturen - zusammengefaßt sind.

BS2000 läuft auf einer Anzahl von verschiedenen Zentraleinheiten, an die wiederum eine Vielzahl von unterschiedlichen Peripheriegeräten angeschlossen werden können. Die HW-Komponenten Zentralprozessor (CPU), Arbeitsspeicher (ASP), Ein-/Ausgabeprozessor mit Kanälen, Plattenspeicher, Bandlaufwerke, Operateurkonsolen, Serviceprozessor (SVP) werden vom Basissystem BASYS betrieben, das somit die wichtigste Brücke zwischen Hardware und Software darstellt. Das Datenfernverarbeitungsnetz, Drucker und Floppy-Disks, "Nichtstandard-Geräte" werden von den Subsystemen DCM bzw. SPOOL bzw. über die Zugriffsmethode ADAM betrieben.

BS2000-SC Version 10.0 ist der um das Sicherheitspaket **SECOS Version 1.0** erweiterte Grundausbau des BS2000 Version 10.0. Dabei sind die **Rechnerkopplung und der Teilhaberbetrieb nicht Bestandteil der F2/Q3-Zertifizierung.**

Mit dem Sicherheitspaket SECOS werden Funktionen zur Verfügung gestellt, die einen Betrieb von BS2000 im Rahmen der F2/Q3-Anforderungen ermöglichen. SECOS besteht aus den Komponenten SRPM, FACS, SAT, SATUT und SATSTAT. Das SRPM-Subsystem SRPMNUC ist Bestandteil des Grundausbaus von BS2000 V10.0.

SRPM (System Resources and Privileges Management) ermöglicht im wesentlichen

- Dezentralisierung von Privilegien der Systemverwaltung, wodurch eine Bündelung oder Entbündelung von deren Aufgaben möglich ist. Die Privilegienvergabe erfolgt durch den Sicherheitsbeauftragten unter einer besonderen Benutzerkennung
- Identifikation und Authentisierung von Benutzern durch erweiterten Zugangsschutz (Batch- und Dialogberechtigung, Berechtigung nur für bestimmte Terminals) und erweiterten Kennwortschutz (Lebensdauerbegrenzung, minimale Länge, Komplexität)
- Einrichtung von Benutzergruppen, mit deren Hilfe ein differenzierter Zugriffsschutz möglich ist. Gruppenverwalter übernehmen dadurch Teile der Systemverwaltungsaufgaben (Bereich Benutzerverwaltung).

FACS (File Access Control System) ermöglicht dem Benutzer durch Einträge in die Zugriffskontrollisten (Access Control List ACL) seiner Dateien, deren Zugriffsschutz bis auf die Ebene von Einzelbenutzern zu regeln.

SAT (Security Audit Trail) ermöglicht Beweissicherung durch Protokollierung sicherheitsrelevanter Ereignisse in eine besonders geschützte Datei (SAT-Logging File). Die SAT-Protokollierung kann nur vom Sicherheitsbeauftragten aktiviert / deaktiviert werden.

Mit Hilfe von SATUT können die SAT-Logging Files von einem autorisierten Benutzer ausgewertet werden.

Mit SATSTAT lassen sich Statistiken über Umfang und Inhalt der Protokolldateien erstellen.

1.1.1 Detaillierte Hardware-Konfiguration

Die von **BS2000 V10.0** unterstützten Geräte sind in den nachfolgenden Tabellen unterteilt in

- Zentraleinheiten
- Geräte mit Gerätetypcode
- Datensichtstationen
- Datenübertragungsvorrechner

- Chipkarten-Geräte
- RSO-Drucker
- Plattenspeichersteuerungen
- ADAM-Geräte.

Da nicht alle von BS2000 V10.0 unterstützten Geräte die Sicherheitsanforderungen an einen F2/Q3-Betrieb erfüllen, ist für jedes Gerät ausgewiesen, ob es zur zertifizierten Konfiguration gehört oder nicht. Sind für den "zertifizierten" Betrieb besondere Maßnahmen zu ergreifen oder Regeln einzuhalten, so wird explizit darauf hingewiesen.

Die **nicht** unter das Zertifikat fallenden Komponenten sind durch **Fettdruck** und Kennzeichnung des Sicherheitsstatus hervorgehoben.

Sicherheitsstatus:

j = Gerät im F2/Q3-Betrieb einsetzbar

n = Gerät nicht für den F2/Q3-Betrieb vorgesehen

1.1.1.1. Zentraleinheiten

Zentraleinheiten	Adressierungsbreite	Sicherheitsstatus
7.500-C40	XS31	j
7.500-H60	XS31	j
7.500-H90	XS31	j
7.500-H120	XS31	j
7.560-EX,FX,HX	XS25	j
7.570-CX,FX,GX,PX	XS25	j
7.580	XS25	j
7.590	XS31	j

Tabelle 1 In V10.0 unterstützte Zentraleinheiten

Anmerkung:

- I/O-Prozessoren und Serviceprozessoren sind integrale Bestandteile der Zentraleinheiten.

1.1.1.2. Geräte mit Gerätetypcode

1. = FAMILY-Code

2. = Gerätekanalklasse

3. = Gerätetypcode

Gerätefamilie	1.	2.	3.	Gerätetyp	Gerätebezeichnung/ Produktnummer	Sicherheits-status
Bedienstation (CONSOLE)	00	S	02	CON3027	BST 3027-1 , -2 BST 3027-101, -102	j j
			03	CON3027C	BST 3027-11 , -21 BST 3027-111, -121 BST 3027-LRC	j j j
		I	**04**	**CON04**	**emulierte 3027-Konsole für ZE mit Bus-Peripherie**	**n**
			0A	CON38	3809/3886 75407-3, -4, -5	j j
			0B	CON3803	75407-1 , 3886-2 ,-3 (Hardcopy am SVP)	j j
			0C	CON3888	Hardcopy 3888-3 (zu NBP 3886) am Clustercontroller 3803-90 75407-1	j j

Gerätefamilie	1.	2.	3.	Gerätetyp	Gerätebezeichnung/ Produktnummer	Sicherheits-status
Schnell-drucker (PRINTER)	20	S	24	PRPND	3350-1 3352-1	j
			26	PRLS333	3337-51 , 3338-51 , -511, -512, -521, -522 3339-51 , -512, -52 , -522	j j j
			27	PRPSHP	3351-21 , -211 3353- 21, -211	j j
			2C	PRL3365	3365-11	j
		I	28	PRPIXH	2090-2 , 2140-2	j
			29	**PRL29**	**Bus-Printer für ZE mit Bus-Peripherie**	**n**
			2A	PRLI333	3338-531, -53, -532 3339-53, -532	j j
			2B	PRPIHP	3351-23, -231 3353-23, -231	j j
			2C	PRL3365	3365-12	j
			2F	PRL3348	3348-120, 3349-120	j
spezielle Geräte (FAM50)	50	S/I	51	DSVP1	SVP-Harddisk	j
		I	**52**	**DSVP2**	**SVP-Harddisk an C40**	**n**
		S	**53**	**TD8170**	**8170-21 (MSN)**	**n**

Gerätefamilie	1.	2.	3.	Gerätetyp	Gerätebezeichnung/ Produktnummer	Sicherheits-status
Datenfern-verarbeitung (TD)	60	S	61	TD960	9631-1 , -2 ,-3	j
			62	ZAS-DUMP	9631-50,-51 ,-52 ,-55	j
			63	ZAS-BCAM		j
			6C	**ZAS-SIN**	**TRANSDATA ZAS mit Anschluß an SINIX**	**n**
			6D	**ZAS-LAN**	**9632-100**	**n**
			6E	**DAST**	**3612**	**n**
		I	61	TD960	9631-1 , -2 ,-3	j
			62	ZAS-DUMP	9631-60,-61 ,-62 ,-65	j
			63	ZAS-BCAM		j
			64	SKP		j
			6D	**ZAS-LAN**	**9632-200**	**n**
			6E	**DAST**	**3801-B**	**n**
physikalisch unterstützte Geräte			71 . . . 7F	"name des exoten-gerätes"	Die Namen werden von ADAM festgelegt. Die Zuordnung zum Gerätetyp-code erfolgt durch die UGEN-Anweisung ADT. ADAM-Geräte siehe Tabelle 8.	
Disketten-geräte (DISKETTE)	90	S	92	FD30243	3171	j 1)
			93	FD3171	3171 mit Zusatz 31712	j 1)
		I	9B	FD75407	75407-2 (C40)	j 1)

1) Die übertragenen Dateien sind mit den Sicherheitsmaßnahmen entsprechend Sicherheitshandbuch für die Systemverwaltung Abschnitt 5.4 zu schützen.

Gerätefamilie	1.	2.	3.	Gerätetyp	Gerätebezeichnung/ Produkt-nummer	Sicherheits-sta-tus
Plattengeräte (DISK)	80/ A0					1)
	80	I	89	D3490-30	3490-3A4,-3A8,-3B4, -3B8,-3BC	j j
			8F	D3475-8F	74305-12 ,-13,-140,-141, -150,-151 (C30)	j j
	A0	S/I	A1	D3439-10	3439-10,-12	j
			A2	D3436	3436, 3436-2,-10,-20	j
			A3	D3437	3437, 3437 -2	j
			A4	D3438-20	3438-20,-22 ,-232	j
		I	A5	D3435	3435 (C40)	j
			A7	D3490-10	3490-1A4,-1A8,-1B4, -1B8,-1BC	j j
		S/I	AB	D3475	3475-1 , -2 ,-3	j
		I	AC	D3480	3410 (externer Schnell-speicher)	j 2)
		S/I	AC	D3480	3480-1, -2 ,-11,-12 , -111,-112 3848-A4,-B4,-AD4,-BD4	j j
			AD	D348E	3480-21 ,-22 3848-AE4,-BE4	j j
		I	AE	D348F	3480-131,-132	j
			AF	D3490-20	3490-2A4,-2A8,-2B4, -2B8,-2BC	j j

1) Diese Geräte sind dann in einem F2/Q3-Betrieb einsetzbar, wenn sie in einem abschließbaren Raum installiert sind.

2) Konfigurationsschalter am Bedienfeld, eine Beweissicherung wird bei Konfigurationsänderung nicht vorgenommen.

Gerätefamilie	1.	2.	3.	Gerätetyp	Gerätebezeichnung/ Produktnummer	Sicherheitsstatus
Bandgeräte (TAPE)	B0/ C0/ E0				Steuerung, + Laufwerk Einheit, + Element +	
unimodale Bandgeräte (UNMTAPE)	B0	S	B2	UM1600	3570 + 3530 3571 + 3531	j j
			B4	UM6250	3513 + 3557, 3559	j 1)
		I	B4	UM6250	3514 + 3557, 3559	j 1)
		S	B7	UM1600-1	3534	j
		I	B9	UMVID-1	MBK2,1 Gbyte Video 8	j
			BA	UMSC-1	MBK 155 Mbyte (nur für SIR und ARCHIVE)	j
Magnetband-kassetten-geräte (MBK)	C0	I	C1	3580	3580-A10 2) +3580-B10 3580-A20 2) + 3580-B20 3590-D31 3590-D32	j j j j
			C2	3590	3580-A10 + 3580-B10 3580-A20 + 3580-B20 3590-D31 3590-D32 3590-A01 + 3590-B02/-B04 3590-A02 + 3590-B02/-B04	j j j j j j
			C4	3590E	3590-D41 3590-D42 3590-A10 + 3590-B20/-B40 3590-A20 + 3590-B20/-B40	j j j j

1) Steuerung für 3557 bzw. 3559, mikroprogrammiert. Mikroprogramm über Magnetbandgerät ladbar, deshalb besondere organisatorische Sicherheitsvorkehrungen für angeschlossene Magnetbandgeräte erforderlich.

2) Mikroprogrammgesteuert, von Diskette ladbar. Steuerung im eigenen Schrank aber unmittelbar neben dem Magnetbandkassettengerät 3580-B10 bzw. 3580-B20 aufzustellen. Besondere organisatorische Sicherheitsmaßnahmen erforderlich.

Gerätefamilie	1.	2.	3.	Gerätetyp	Gerätebezeichnung/ Produktnummer		Sicherheitsstatus
Bandgeräte (TAPE)	B0/ C0/ E0				Steuerung, Einheit, Element	+ Laufwerk + +	
bimodale Bandgeräte (BIMTAPE)	E0	S	E2	BM1662	3513	+ 3557, 3559	j 1)
		I	E2	BM1662	3514	+ 3557, 3559	j 1)
		S	E2	BM1662	3515	+ 3525	j
					3516	+ 3526	j
					3517-1	+ 3527-1	j
					3519	+ 3529	j
					3535	+ 3525	j
					3536	+ 3526	j
					3537-1	+ 3527-1	j
		I	E2	BM1662	3517-3	+ 3527-3	j 2)
					3519-3	+ 3529	j 2)
		S	E3	BM1662S	3518	+ 3528	j
					3538	+ 3528	j
		I	E4	BM1662S1	3506 (C40)		j
			E8	BM1662FS	3504-625		j

Tabelle 2 Geräte mit Gerätetypcode und Sicherheitsrelevanz

1) Steuerung für 3557 bzw. 3559, mikroprogrammiert. Mikroprogramm über Magnetbandgerät ladbar, deshalb besondere organisatorische Sicherheitsvorkehrungen für angeschlossene Magnetbandgeräte erforderlich.

2) Steuerung integriert und über Diskette ladbar. Besondere organisatorische Sicherheitsmaßnahmen erforderlich.

Gerätekanalklassen:

S: Blockmultiplexkanal Typ 1 (SBL) oder Bytemultiplexkanal Typ 1 (SBY)

I: Blockmultiplexkanal Typ 2 (IBL) oder Bytemultiplexkanal Typ 2 (IBY) oder Emulation des Multiplexkanal Typ 2 (Buskanal)

Plattengeräte sind immer an Blockmultiplexkanäle angeschlossen. Magnetbandgeräte können an Block- und an Bytemultiplexkanäle angeschlossen sein.

1.1.1.3. Datensichtstationen

Datensichtstationen	Sicherheitsstatus
9755	j
9758	j
9762	j
9763 (für Chipkarte erforderlich) 1)	j
9756 Monochrom	j
9756-1	j
9756-5	j
9756-11	j
9756-31	j
9758-M Monochrom	j
9762-C Colour	j
9763-M Monochrom	j
9763-C Colour	j
9763-G Grafik Colour	j

Tabelle 3 In V10.0 unterstützte Datensichtstationen mit Sicherheitsrelevanz

1) Im F2/Q3-System einsetzbar, wenn Diskettenlaufwerk versiegelt wird oder wenn Korrektheit der Software anderweitig sichergestellt werden kann.

Anmerkung:
Im zertifizierten System BS2000-SC V10.0 dürfen ausschließlich die in Tabelle 3 aufgeführten Datensichtstationen eingesetzt werden.

1.1.1.4. Datenübertragungsvorrechner

Datenübertragungsvorrechner	Sicherheitsstatus
9681-1 , -2, -2U	j
9686-1 , -1U, -2, -2U	j
9687-12 , -120, -14	j
9688-1 , -2, -3, -3U	j
75409-1, -2	j

Tabelle 4 In V10.0 unterstützte Datenübertragungsvorrechner mit Sicherheitsrelevanz

1.1.1.5. Chipkarten-Geräte

Chipkarten-Geräte	Sicherheitsstatus
Chipkarte V1.0	j
Chipkarte V2.0	j
Chipkartenterminal (CKT)	j
Chipkartenleser (CKL)	j
Zentrales Autorisierungsterminal ZAT2000 mit Sicherheitsmodul SM2	j

Tabelle 5 In V10.0 unterstützte Datenübertragungsvorrechner mit Sicherheitsrelevanz

1.1.1.6. RSO-Drucker

RSO-Drucker	Sicherheitsstatus
9001-N	j
9002	j
9003	j
9004	j
9011-N	j
9012	j
9013	j
9014	j
9020	j
9021	j
9022	j
9023	j
9025-1	j
9025-2	j
9025-3	j
9025-10	j
9025-102	j
9026	j
9046	j
9047	j
9645-7	j
9645-8	j
DJET } Drucker-	j
LJII } schnittstellen	j

Tabelle 6 In V10.0 unterstützte RSO-Drucker mit Sicherheitsrelevanz

1.1.1.7. Plattenspeichersteuerungen

Plattenspeichersteuerungen	Sicherheitsstatus
3410	j 1)
3418-11	j 2) 3)
3418-111	j 2) 3)
3418-121	j 2) 3)
3418-13	j 2) 3)
3418-21	j 2) 3)
3418-22	j 2) 3)
3418-23	j 2) 3)
3418-42	j 2) 3)
3419-23	j 1) 4)
3419-43	j 1) 4)
3860-2	j 1) 4)
3860-30	j 1) 4)
3860-31	j 1) 4)
3860-41	j 1) 4)
3860-42	j 1) 4)
75403-1	j 5)
75603-1	j 6)
75605-2	j 7)

Tabelle 7 In V10.0 unterstützte Plattenspeichersteuerungen mit Sicherheitsrelevanz

1) Konfigurationsschalter am Bedienfeld, eine Beweissicherung wird bei Konfigurationsänderung nicht vorgenommen.

2) Konfigurationsmöglichkeit über SVP, Bewertung bezüglich Beweissicherung wie Zentraleinheit.

3) Die Firmware dieser Plattensteuereinheit wird über den SVP geladen. Die Sicherheitsbewertung dieser Steuerung ist daher die der Zentraleinheit, in die der SVP integriert ist.

4) Die Firmware ist an den Steuerungen ladbar bzw. austauschbar. Die Geräteschutzverkleidung kann mit Hilfe eines Sechskantschlüssels entfernt werden. Es ist deshalb zu garantieren, daß die Geräteverkleidung mit einem Sicherheitsschloß versehen wird oder daß dieses Gerät in einem abschließbaren Raum installiert wird.

5) Bestandteil von C40, Sicherheitsbewertung wie Zentraleinheit.

6) Bestandteil von 7.560, Sicherheitsbewertung wie Zentraleinheit.

7) In Zentraleinheit eingebaute 3418-21 , Sicherheitsbewertung wie 3418-21.

1.1.1.8. ADAM-Geräte

ADAM-Geräte	Sicherheitsstatus
Markierungsblattleser 4264 und 3262	j
Lochstreifenleser 4229 und 4223	j
Lochstreifenstanzer 4228	j
Floppy-Disk-Gerät Ressmann	j
Floppy-Disk-Gerät Ressmann (I-Kanal)	j
Prüfautomat für Logikbaugruppen PALOG-B 560	j
Plotter BENSON 1330	j
Plotter BENSON 936 QADRAMET	j
Lichtsetzmaschine DIGISET	j
Lochkartenleser 4239, 4235 und 3150	j
Lochkartenstanzer 4238 und 3160	j
Schaltereinheit 3070	j
Datenaustauschsteuerung 627	j
Floppy-Disk-Geräte 317X und 302XX	j
Floppy-Disk-Gerät F443 (I-Kanal)	j
Mechanikdrucker ohne Formularkontrollpuffer	j
Mechanikdrucker 333X mit Formularkontrollpuffer	j
Mechanikdrucker 3339 mit Formularkontrollpuffer (I-Kanal)	j
Plattenspeicher IBM 3380 (I-Kanal)	j
Scientific Computer FPS-364 (I-Kanal)	j
ZYCAD Logical Evaluator (I-Kanal)	j
Adapter NSC HYPER-CHANNEL	j
Adapter NSC HYPER-CHANNEL (I-Kanal)	j
ETHERNET Verbindung für lokale Netze (I-Kanal)	j
Kassettengerät MULTISTREAM 300	j
Kassettengerät MULTISTREAM 300 (I-Kanal)	j
Datenbank-Rechner DBC/1012	j
Drucker 333X mit Formularkontrollpuffer	j
Drucker 333X mit Formularkontrollpuffer (I-Kanal)	j
SVP Hard-Disk	j
SVP Hard-Disk (I-Kanal)	j
SVP Hard-Disk (I-Kanal/ C40)	j
ZAS / Laden und Dump	j
ZAS / Laden und Dump (I-Kanal)	j
Anschlußsteuerung für LOCAL AREA NETWORK	j
Anschlußsteuerung für LOCAL AREA NETWORK (I-Kanal)	j
C40-Floppy-Disk	j

Tabelle 8 Im F2/Q3-Betrieb über ADAM anschließbare Gerätetechnik

Anmerkung:

Sollen im F2/Q3-Betrieb weitere Geräte über ADAM angeschlossen werden, so ist dies nur mit einer sicherheitsbewerteten und vom Hersteller ausgelieferten ADAM-Gerätetabelle möglich.

1.1.2 Detaillierte Software-Konfiguration

Die folgenden Tabellen weisen den Sicherheitsstatus von BS2000-Produkten aus.

Dieser Anhang besteht aus zwei Teilen:

I. "BS2000-Grundausbau aus sicherheitstechnischer Sicht"

II. "Ausgewählte Teile der im Vertriebshandbuch ausgewiesenen BS2000-Produkte aus sicherheitstechnischer Sicht"

Definition der Sicherheitsgruppen für die Software-Bestandteile:

Gruppe A Software-Bestandteile, die das F2/Q3-System bilden

Gruppe B Software-Bestandteile, die unter Steuerung des F2/Q3-Systems sicher ablaufen, aber nicht evaluiert werden müssen, da sie die Sicherheitsstufe des Systems nicht verändern können.

Gruppe D Gegenwärtig nicht sicherheitsbewertete Produkte, die im zertifizierten System nicht eingesetzt werden können

Gruppe D* Gegenwärtig nicht sicherheitsbewertete Produkte, die im zertifizierten System nicht eingesetzt werden können, da sich das F2/Q3- Zertifikat nur auf den Betrieb eines Einzelsystems bezieht

Produkte der Gruppen D und D* sind im folgenden durch Fettdruck hervorgehoben.

Teil I: BS2000-Grundausbau aus sicherheitstechnischer Sicht:

Nr.	Bestandteil		Sicherheits-Gruppe	Bemerkung
	Name	Version		
1	ADAM	10.0A	A	
2	AIDSYS	10.0A	A	
3	ANITA	10.0A	A	
4	ASSGEN	0.4A	B	Produktionstool; muß im F2/Q3-System angewendet werden.
5	BINDER	1.0A	B	
6	BLSSEC	10.0A	A	
7	BS2CP	10.0A	A	
8	DAMP	2.0C	B	
9	DPAGE	10.0A	B	
10	DSSM	2.0A	A	
11	DSSMGEN	2.0A	B	Produktionstool; muß im F2/Q3-System angewendet werden.
12	ELFE	10.0A	B	

Nr.	Bestandteil		Sicherheits-Gruppe	Bemerkung
	Name	Version		
13	ELS	10.0A	B	
	ELS	10.0B	B	
	ELP	10.0A	B	
	ELP	10.0B	B	
	ELT	10.0A	B	
	ELT	10.0B	B	
14	GET-TIME	10.0A	A	
15	**IDA**	**10.0A**	**D**	
16	INIT	10.0A	A	
17	IOCFCOPY	2.0A	A	
18	JMS	10.0A	A	
	JCGEN	**10.0A**	**D**	
	JMU	10.0A	B	
	JOBSCHED	10.0A	A	
19	LLMAM	1.0A	B	
20	LMSCONV	1.0A	B	
21	MSGEDIT	11.8D	B	
22	MSGLIB	15.2D	B	
23	**NDCATOP**	**10.0A**	**D**	
24	NDM	10.0A	A	
	NKS	10.0A	A	
	NKV	10.0A	A	
25	NKISAM	10.0A	A	
26	**PAMCONV**	**10.0A**	**D**	
27	PAMINT	1.0B	B	
28	PASSWORD	1.0A	B	
29	**PDPOOLS**	**10.0A**	**D**	
30	PLAM	1.5A	A	
31	**PPD**	**10.0A**	**D**	
32	**PVSREN**	**1.0A**	**D**	
33	**RECAT**	**10.0A**	**D**	
34	RFUPD	1.3B	B	
35	RMS	6.0A	B	
36	**SAVECAT**	**10.0A**	**D**	
37	**SDF**	**1.4A**	**D**	
	SDF	1.4B	A	
38	SDF-I	1.1A	B	
	SDF-I	1.2A	B	
39	SDF-U	1.0D	B	
40	SDFSYS	1.7A	A	

Nr.	Bestandteil		Sicherheits-Gruppe	Bemerkung
	Name	Version		
41	SHOW-FILE	10.0A	A	
42	**SINIX-2000**	**10.0A**	**D**	
43	SIR	2.0A	A	
	BSIR	2.0A	A	
44	SJMSAVE	10.0A	B	
45	SKP	1.0A	A	
	TELESERVICE	1.0A	A	
46	SODA	10.0A	B	
47	**SPCCNTRL**	**10.0A**	**D**	
48	**SPOOL**	**2.5A**	**D**	
	FDEXIM	1.5A	B	
	FDRIVE	1.1B	B	
	PRSERVE	1.2E	B	
	SPOOLSERVE	1.5A	B	
	SPSERVE	1.5A	B	
	SPOOL	2.5B	A	
	FDEXIM	1.5A	B	
	FDRIVE	1.1B	B	
	PRSERVE	1.2F	B	
	SPOOLSERVE	1.5B	B	
	SPSERVE	1.5B	B	
49	SRPSAVE	10.0A	B	
50	STARTUP	10.0A	A	
	BOOT	10.0A	A	
	HR$F	10.0A	A	
	HR$X	10.0A	A	
	HR$6	10.0A	A	
	IPL	10.0A	A	
	SLED	10.0A	A	
	STRT	10.0A	A	
51	SYSFILE	10.0A	A	
52	**SYSTEM-EXITS**	**10.0A**	**D**	
53	**SYSUPD**	**10.0A**	**D**	
54	TPCOMP2	10.0A	B	
55	TSOSLNK	21.0C	B	
	TSOSLNK	21.0D	B	
56	**TSOSMT**	**10.0A**	**D**	**nur auf Diagnoseband**
57	UGEN	10.0A	B	Produktionstools; müssen im
	IOCGEN	10.0A	B	F2/Q3- System angewendet werden.
58	VOLIN	10.0A	A	

Tabelle 9:BS2000-Grundausbau aus sicherheitstechnischer Sicht

Teil II: Ausgewählte Teile der im Vertriebshandbuch ausgewiesenen SNI-Produkte aus sicherheitstechnischer Sicht

Nr.	Bestandteil		Sicherheits-Gruppe	Bemerkung
	Name	Version		
1	**ACUT**	**4.0B**	**D**	**nur auf Vorrechner**
2	ADA	2.0A	B	
	ADA	2.0B	B	
3	ADIAG	30.0A	B	
4	ADILOS	6.0A	B	
	ADILOS-DB	6.0A	B	
	ADILOS-DVS	6.0A	B	
5	AID	1.0C	A	
	AID	**2.0A**	**D**	
6	APLX	1.0D	B	
7	APLX-FS	1.0D	B	
8	AP210	2.0D	B	
9	**ARCHIVE**	**2.7A**	**D**	
	ARCHIVE	2.7B	A	
10	ARITHMOS	1.0A	B	
	ARITHMOS	1.1A	B	
11	ASECO	1.0A	A	
12	ASSEMBH	1.0A	B	
13	AVAS	1.0A	B	
	AVAS-RG	1.0A	B	
	AVAS-PROG	1.0A	B	
	AVAS	1.1A	B	
	AVAS-RG	1.1A	B	
	AVAS-PROG	1.1A	B	
14	C	1.0A	B	
	C	1.0B	B	
	C	2.0A	B	
15	COBOL85	1.0A	B	
	COBOL85	1.1A	B	
16	COB	2.3A	B	
17	COLUMBUS-ASS	2.2F	B	
18	**COSMOS**	**10.0A**	**D**	
	CAP	**10.0A**	**D**	
	NEGET	**10.0A**	**D**	
19	DAB	3.5A	A	
20	**DCADITO**	**10.0A**	**D**	

Nr.	Bestandteil		Sicherheits-Gruppe	Bemerkung
	Name	Version		
21	DCM	10.0A	A	
	BCAM	10.0A	A	
	BCAM-LTS	**9.3A**	**D**	
	BCAM-LTS	**10.0A**	**D**	
	DCAM	10.0A	A	
	RBAM	**8.9A**	**D**	
	RBAM	**10.0A**	**D**	
	TIAM	10.0A	A	
	VTSU-B	9.0B	A	
22	**DFS**	**1.0A**	**D**	
23	**DORA**	**2.0A**	**D**	
	DORA	**2.0B**	**D**	
24	DRIVE	5.2A	B	
	DRIVE	6.0A	B	
25	DRIVE-COMP	1.0A	B	
26	DRV	1.0A	A	
27	EDOR	8.3D	B	
28	EDT	16.2A	B	
	EDT	16.3A	B	
29	FDDRL	10.0A	A	
30	FHS	6.0B	B	
	FHS	7.0A	B	
31	FMS	2.4A	B	
32	FOR	2.1A	B	
	FOR	2.2A	B	
33	**FOR77VP**	**1.1A**	**D**	
34	**FT-BS2000**	**4.0B**	**D***	
35	**FTAC-BS2000**	**1.0B**	**D***	
	FTAC-BS2000	**1.0C**	**D***	
36	**GOLEM**	**7.0A**	**D**	
	GOLEM	**7.1A**	**D**	
37	**HELGA**	**16.2H**	**D**	
38	**HSMS**	**1.1A**	**D**	
	HSMS	**1.2A**	**D**	
39	**IDIAS**	**1.8A**	**D**	
40	**IFG**	**5.0A**	**D**	
	IFG	**6.0A**	**D**	

Nr.	Bestandteil		Sicherheits-Gruppe	Bemerkung
	Name	Version		
41	IGS	1.1A	B	
42	IOTRACE	10.0A	A	
43	IQS	3.1D	B	
44	JV	10.0A	A	
45	LEASY	5.1A	B	
46	LISP-SCL	1.0A	B	
47	LMS	1.4A	B	
	LMS	2.0A	B	
48	LPS	1.1A	B	
49	MAREN	5.0A	A	
50	**MSCF**	**10.0A**	**D***	
51	NKGDUMP	10.0A	B	Benötigt Lese-/Schreibprivilegierung 8/8, da sonst nur beschränkt einsetzbar.
52	**NKISTRAC**	**10.0A**	**D**	
53	**NLMSERVE**	**10.0A**	**D**	
54	**NTAC2**	**5.0A**	**D**	
	NTAC2	**5.0B**	**D**	
	NTAC2	5.0C	A	
55	**NTAC2E**	**3.0B**	**D**	
	NTAC2E	3.0C	A	
56	**OKTOPUS**	**1.0A**	**D***	
57	**OMNIS**	**6.1B**	**D**	
	OMNIS	**6.1C**	**D**	
	OMNIS	6.1D	A	
	OMNIS	**6.2A**	**D**	
58	**OMNIS-MENU**	**1.0A**	**D**	
	OMNIS-MENU	**1.1A**	**D**	
59	**OMNIS-PROP**	**3.1A**	**D**	
60	**OSS**	**2.0A**	**D**	
	OSS	**2.0B**	**D**	
61	**PASCAL**	**3.1C**	**D**	
62	PASCAL-XT	2.0A	B	
	PASCAL-XT	2.0B	B	
	PASCAL-XT	2.1A	B	
63	PASSAT	6.1A	B	
64	**PCS**	**2.0A**	**D**	

Nr.	Bestandteil		Sicherheits-Gruppe	Bemerkung
	Name	Version		
65	**PDN-GA**	**9.0A**	**D**	
	PDNGEN	**9.0A**	**D**	
	PDN-GA	**10.0A**	**D**	
	PDNGEN	**10.0A**	**D**	
	PDN-GA	10.0B3	A	
	PDNGEN	10.0B	B	Produktionstool; muß im F2/Q3-System angewendet werden.
66	PERCON	2.4A	B	
67	**PETRA**	**10.0A**	**D**	
68	PLI	4.0A	B	
	PLI	4.0C	B	
	PLI	4.1A	B	
69	**PRISMA**	**4.5A**	**D**	
70	PROLOG	1.0A	B	
	PROLOG	2.1A	B	
71	**PROP-PPM**	**1.0A**	**D***	
	PROP-PPM	**2.0A**	**D***	
72	**PROP-TPM**	**1.0A**	**D***	
73	**PROP-XAF**	**1.0A**	**D***	
74	QUERY	1.0A	B	
75	RAV	1.1A	B	
76	RESY	1.0A	B	
77	**RFA**	**10.0A**	**D***	
78	**ROBAR**	**2.0A**	**D***	
79	**ROSI**	**10.0A**	**D**	
80	RPG3	2.0A	B	
	RPG3	2.0B	B	
	RPG3	3.0A	B	
81	**RSO**	**2.1A**	**D**	
	RSOSERVE	**2.1A**	**D**	
	RSO	2.1B	A	
	RSOCONV	2.1B	B	
	RSOSERVE	2.1B	B	
82	SCA	10.0A	A	
83	SDF-A	1.0D	B	
84	SECOS	1.0A	A	
	FACS	1.0A	A	
	SATCP	1.0A	A	
	SATUT	1.0A	A	
	SRPMOPT	1.0A	A	

Nr.	Bestandteil		Sicherheits-Gruppe	Bemerkung
	Name	Version		
85	SESAM	14.1A	B	
86	SESAM/SQL	1.0A	B	
87	**SM2**	**10.0A**	**D**	
88	**SM2-IBIS**	**2.0A**	**D***	
89	**SM2-PA**	**1.0A**	**D**	
90	SORT	7.3A	B	
91	SPL	1.4C	B	
	SPL	1.5B	B	
	SPL	1.6A	B	
92	TDA	3.0B	B	
	TDA	3.0C	B	
93	TDDIAG	1.0C	B	
94	UDS/SQL	1.0A	B	
95	**UTM**	**3.1A**	**D**	
	UTM	**3.2A**	**D**	
96	**UTM-D**	**1.1A**	**D***	
	UTM-D	**1.2A**	**D***	
97	UX-BASIC	2.1A	B	
	UX-BASIC	3.0A	B	
98	**VM2000**	**1.2A**	**D**	
99	**VTSU-X.29**	**1.2A**	**D**	
100	**XAF**	**2.0A**	**D**	

Tabelle 10 Ausgewählte Teile der im Vertriebshandbuch ausgewiesenen SNI-Produkte aus sicherheitstechnischer Sicht

1.2 Liste der zum evaluierten System gehörigen Anwenderdokumentation

Folgende Manuale, die die Anwendung der Sicherheitsfunktionen des BS2000-SC V10.0 beschreiben, sind beim Hersteller beziehbar. Darüber hinaus stehen für die nicht sicherheitsrelevanten Produkte weitere Manuale zur Verfügung, die beim Hersteller bezogen werden können.

- BS2000 V10.0A, Sicherheitshandbuch für die Systemverwaltung, U5627-J-Z125-1
- BS2000 V10.0A, Sicherheitshandbuch für den Benutzer, U6521-J-Z125-1
- BS2000 V10.0A, Systembedienung, U2000-J-Z125-7
- BS2000 V10.0A, Systeminstallation, U2505-J-Z125-10
- BS2000 V10.0A, Systemverwaltung, U2417-J-Z125-9
- SECOS V10.0A, Benutzerhandbuch, U5605-J-Z125-1
- MAREN V5.0, Benutzerhandbuch, U2106-J-Z87-3
- TRANSDATA Netzmanagement, Benutzerhandbuch, NTAC2 V5.0C, NTAC2E V3.0C, DCAM V10.0A, U1632-J-Z135-8

2. Sicherheitsanforderungen

2.0 Systemüberblick über die Grundversion BS2000 V10.0

BS2000 ist ein Universal-("General-Purpose")-Betriebssystem, das den Teilnehmerbetrieb mit den Betriebsarten Stapel- und Dialogbetrieb sowie den Teilhaberbetrieb mit den Betriebsarten transaktionsorientierter Betrieb und freier Anwendungsbetrieb unterstützt.

Diese Betriebsarten können sowohl unabhängig voneinander als auch kombiniert auf einem Rechensystem genutzt werden. Der Teilnehmerbetrieb umfaßt die Abwicklung von Stapel- und Dialogaufträgen. Ein Auftrag besteht aus einer Folge von Aufrufen von Funktionen des Systems über die Kommandosprache.

Im Teilhaberbetrieb nutzt eine Anwendung oder ein Anwendungssystem als Benutzerprogramm die Funktionen des Betriebssystems und seiner höheren Subsysteme und stellt selbst Funktionen für sog. Endbenutzer zur Verfügung.

Die Tätigkeit des Planens und Steuerns gemäß strategischen und sicherheitspolitischen Vorgaben ist Aufgabe der Systemverwaltung. Die Aufgaben der Systemverwaltung können auf mehrere weitgehend voneinander unabhängige Rollen aufgeteilt werden.

Laufende Überwachungs- und Steuerungstätigkeiten werden weitgehend durch die Systembedienung wahrgenommen. Ausgenommen hiervon sind die Aufgaben, die wegen ihrer zentralen Bedeutung für den Betrieb des BS2000 nur von der Systemverwaltung durchgeführt werden können.

Das BS2000 besteht aus einer Anzahl von Subsystemen als einer Menge ausgezeichneter Funktionseinheiten. Subsysteme sind Einheiten der Montage und der Installation und werden aus Programmbausteinen montiert, die entweder einzelne Komponenten sind oder eine vormontierte oder logisch zusammengehörige Komponentengruppe bilden.

Zugeordnet zu Subsystemen sind sog. Nebenkomponenten, wie Kommandosyntaxbeschreibungen (Syntax-Files), Meldungstextdateien (Message-Files) und generative Komponenten, die von anderen Subsystemen zur Benutzung der angebotenen Programmierschnittstellen benötigt werden (z.B. Schnittstellen-Makros und sog. Includes).

Abhängig davon, ob sie im vorgenerierten Ladesystem vorhanden sein müssen oder nicht, sind Subsysteme in obligate und optionale unterteilt. Einige Subsysteme können ihrerseits untergeordnete Funktionseinheiten oder einzelne Programmbausteine erst bei Bedarf vom Peripheriespeicher laden.

2.1 Sicherheitsphilosophie

2.1.1 Sicherheitsgrundsätze im BS2000-SC Version 10.0

Die Abkürzung BS2000 wird im folgenden für das zertifizierte System verwendet.

Die Sicherheitsgrundsätze des BS2000 legen fest, wie es durch Personen benutzt werden kann, und welche Möglichkeiten der Betreiber des BS2000 hat, die Nutzungsmöglichkeiten zu steuern, zu regeln und zu überwachen. Die dabei aus dem potentiellen Einsatz stammenden Bedrohungen sind:

B.1: Zugang unberechtigter Personen zum System,

B.2: Unbefugte Ausübung von privilegierten Tätigkeiten,

B.3: Unbefugter Zugriff auf Betriebsmittel und auf gespeicherte Information

B.4: Fahrlässige und mißbräuchliche Nutzung von Privilegien,

B.5: Fehlfunktionen des Systems,

B.6: Fehlbedienung durch Systemadministration oder Benutzer

B.7: Verfälschung des Systemcodes oder zentraler Systemdaten

Alle diese Bedrohungen haben gleichermaßen Bezüge zu den drei Grundbedrohungen

- Verlust der Vertraulichkeit,
- Verlust der Integrität,
- Verlust der Verfügbarkeit (denial-of-service).

Üblicherweise entsprechen den natürlichen Personen (Subjekte außerhalb des BS2000) mehrere Subjektbegriffe innerhalb des BS2000. Zur Beschreibung prinzipieller Beziehungen von Subjekten untereinander und prinzipieller Nutzungsmöglichkeiten von Objekten wird systemintern eine Beschreibung von Repräsentanten der Benutzer (Benutzerkennung, User-id) gehalten. Jeder Vorgang (Benutzerauftrag, Job; Taskprozeß etc.), der dann gestartet wird, wird einem so beschriebenen "Benutzer" zugeordnet und die ihm möglichen Beeinflussungsmöglichkeit anderer Vorgänge bzw. Nutzungsmöglichkeiten von Objekten werden entsprechend den in bezug auf "Benutzer" gemachten statischen Vorgaben begrenzt.

Eine wesentliche Leistung des BS2000 zur Abwehr von B.1, B.2, B.3 ist deshalb, die Zuordnung von natürlichen Personen zu ihren systeminternen Repräsentanten sicherzustellen, diese auf aktive Subjekte zu übertragen und dem Benutzer entsprechende Steuerungsmöglichkeiten zu geben, Objekte mit anderen Benutzern gemeinsam nutzen zu können.

Da das BS2000 einerseits die hierzu benötigten Steuer- und Regelvorgaben sicherstellen muß, andererseits erlaubt, diese weitgehend flexibel zu ändern, spielt das Zusammenwirken zwischen den Subjekten im BS2000 und dem BS2000 als Ganzem eine Rolle. Das BS2000 muß sicherstellen, daß Regelvorgaben für Subjekte nicht umgangen und nur kontrolliert verändert werden können. Darüber hinaus kann es wünschenswert sein, daß für ein fest generiertes und installiertes System gewisse Regelvorgaben nur beschränkt durch den Betreiber verändert werden können.

Zur Abwehr von B.7 muß der Betreiber vorrangig ein unverfälschtes BS2000 installieren, sein eigenes Wohlverhalten ist hierfür Voraussetzung. Veränderungen des Systems selbst werden im Rahmen des geregelten Betriebs ausgeschlossen, gewisse Sicherheitsgarantien werden durch Wahl spezieller Generierungsoptionen gegeben. Durch Loggingverfahren wird die Voraussetzung für einen revisionsfähigen Betrieb geschaffen. Das System enthält Funktionen, um auch bei externen und internen Störungen den Betrieb aufrechtzuerhalten. Die im laufenden Betrieb möglichen Änderungen durch die Administration und die Operateure können allerdings immer noch zur Verfälschung des Systems führen, wenn nicht besondere Vorkehrungen insbesondere zur Abwehr von B.4 und B.2 getroffen werden. Erst wenn alle Vorkehrungen wirksam werden, ist für die geregelte Kooperation von Benutzern im System eine sichere Umgebung geschaffen.

2.1.2 Voraussetzungen für den "sicheren" Betrieb

Auslieferung und Installation

Für den "sicheren" Betrieb sind die Installierung eines unverfälschten Systemcodes sowie dessen richtiger (statischer, dynamischer) Parameterisierung und sein Arbeiten über zuverlässig erstellte Steuerdateien für Subsysteme primäre Bedingungen. Ihre Erfüllung obliegt dem Betreiber (zur Abwehr von B.7).

Hierbei bestehen für den Betreiber verschiedene Optionen, die im "Sicherheitshandbuch für den Systemverwalter" detailliert beschrieben sind. Insbesondere erfordert ein F2/Q3-System die Wahl spezieller Systemparameter.

Unverfälschter Systemcode

Generiert der Betreiber den Systemcode aus Komponenten und Nebenkomponenten, die er vom Hersteller übernommen hat, so muß für das generierte System dessen unverfälschte Zusammensetzung überprüft werden:

- Verwendung nur von Originalkomponenten.
- Einspielen nur von offiziell validierten Korrekturen (REPs, etc.).
- Einstellen der gewünschten Systemoptionen.
- Bereitstellung eines Subsystemkatalogs mit Bezügen zu Originalsubsystemen des BS2000.
- Generierung der zur Software passenden Hardware-Konfiguration der Peripherie.
- Bereitstellen von Dateien für die Parametrisierung der Systeminbetriebnahme (Startup-Parameter-Service).
- Bereitstellen von Steuerdateien für die Subsysteme
- Bereitstellen von Dateien als Behälter für eventuell anfallende Diagnoseinformationen (SLED-, SNAP-Datei).
- Generierung des Datenfernverarbeitungssystems (TRANSDATA-PDN) ausschließlich zur Bedienung von Datensichtgeräten.

Ein generiertes System kann auf Basis der Generierungsunterlagen einem Plausibilitätstest auf seine Korrektheit unterzogen werden. Auch bei Erstinstallation kann nach einem Zwischenschritt über das sog. "selbstladende" Produkt SIR die Generierung über BS2000 kontrolliert erfolgen (zur Abwehr von B.7).

Kontrolle von Installationsänderungen

Um einen 24-Stundenbetrieb organisieren zu können, wird eine Änderung der installierten Softwarekonfiguration im laufenden Betrieb geboten. Diese beschränkt sich auf einzelne ausgewählte Subsysteme, die entladen und/oder hinzugefügt werden können und als solche besonders im Systemkatalog gekennzeichnet sind. Kritisch sind hierbei solche Subsysteme, die mit System-Privileg ablaufen oder die von einer privilegierten Systemverwalterkennung eingesetzt werden. Verantwortlich für die korrekte Subsystemkonfiguration ist der Systemverwalter und der Operateur, dessen Tätigkeit über das CONSLOG-Protokoll kontrolliert werden kann (zur Abwehr von B.4, B.6 und B.7).

Bei schwerwiegenden Systemfehlern und/oder aufgrund der Entscheidung des Operateurs wird ein Systemlauf abgebrochen. Es kann dann ein SLED-Dump als Unterlage für eine nachfolgende Diagnose erstellt werden, und ein neuer Systemlauf begonnen werden. Aufgrund der CONSLOG- Protokolle zu den zugehörigen Systemläufen kann dieses Ereignis erkannt und nachgeprüft werden, ob die Referenzen zu Systemcode, Parameterisierung oder Steuerdateien gewechselt wurden (zur Abwehr von B.4 und B.7). Unter der Voraussetzung, daß die zugehörigen Dateien unverfälscht geblieben sind, kann eine unentdeckte Verfälschung des installierten Systems ausgeschlossen werden.

Separierung des Systems

Ein unverfälschtes BS2000 bietet die Schutzfunktionen, auf deren Basis der Betreiber und der einzelne Benutzer einen "sicheren" Betrieb organisieren kann (zur Abwehr von B.7 im laufenden Betrieb).

Schutz des Systems gegen Veränderungen und Störungen

BS2000 bietet mit den als privilegiert ablaufenden Subsystemen eine vertrauenswürdige Basis für alle Zugriffe durch Programmläufe des Benutzers auf die vom BS2000 geschützten Objekte. Der Schutz der Speicherbereiche (Separierung der evaluierten Systemteile) ist nach dem Schloß-Schlüsselprinzip realisiert durch ein Speicherschloß, das jeder Seite im Hauptspeicher zugeordnet ist, und einem vom System eingestellten Ablaufschlüssel für Programmläufe. Nur privilegierte Subsysteme setzen selbst

Speicherschlösser und Ablaufschlüssel. Dabei wird sichergestellt, daß nicht privilegiert ablaufende Programme immer mit einem nichtprivilegierten Schlüssel ablaufen, so daß sie auf die vom BS2000 benutzten privilegierten Speicherseiten nicht zugreifen können.

Wird ein Systemdienst von Programmläufen des Benutzers aufgerufen, so kann dies nur über die Schnittstelle SVC (Supervisor Call) erfolgen. Hierbei werden alle Parameter auf ihre Gültigkeit überprüft.

Schutz der sicherheitsrelevanten Aufträge und Auftragsdaten

Verschiedene Benutzeraufträge werden getrennten Adreßräumen zugeordnet. Nur über Objekte (Dateien, Memorypools, Event-Items), deren gemeinsame Nutzung von allen Partnern gezielt - zum Zwecke einer Kooperation - organisiert wird, ist eine wechselseitige Beeinflussung oder Störung möglich. Aufträge der Systemadministration können deshalb vollständig geschützt vor Störungen durch Aufträge anderer Benutzer ablaufen, indem sie auf eine Kooperation mit diesen verzichten.

Die zu diesen Aufträgen gehörenden Daten werden dadurch geschützt, daß auf sie nur von entsprechend privilegierten Benutzerkennungen zugegriffen werden kann. Hierzu gehören insbesondere der zentrale Datei- und Jobvariablen-Katalog, in dem die Eigentümerschaft von Dateien und Jobvariablen verzeichnet ist, sowie die SRPM-Datei, die alle Rechte und Privilegien von Benutzerkennungen enthält.

Für die SRPM-Datei besteht noch ein Schutz über die privilegierte Eigentümerschaft hinaus: auf sie kann während des Betriebs von keinen Aufträgen unter Umgehung der SRPM-Task zugegriffen werden, auch nicht von privilegierten Benutzern.

Schutz von Daten des Betreibers gegen Zugriffe des Bedien- und des Wartungspersonal

Durch die Generierungsoption der Paßwort-Verschlüsselung (Logon-, Datei- und JV-Paßwörter) mit einer Einwegfunktion sind diese sicherheitskritischen Daten auch aus Diagnoseunterlagen i.a. nicht gezielt zu entnehmen. Ausnahmen sind kurzfristige Phasen zwischen Eingabe und Verschlüsselung, in denen unverschlüsselte Paßwörter in einen von außen provozierten Systemdump gelangen können.

Operateure haben keinen direkten Zugriff auf Dateien und Jobvariable im System. Sie können allenfalls vorbereitete Aufträge (auch unter Benutzerkennungen der Systemverwaltung) starten und über diese mittelbar Dateien und Jobvariable bearbeiten. Ein direktes Abfragen von Inhalten der bearbeiteten Dateien durch Operateure wird dabei ausgeschlossen (zur Abwehr von B.3).

Über eine ausgezeichnete Benutzerkennung (SERVICE) kann der Betreiber Zugriffe auf Prüfdaten und ausgewählte Dateien durch den Wartungstechniker erlauben. Die Testdaten sind durch die zum Ablauf gebrachten Prüfprogramme vorgegeben und müssen sich dazu im Betrieb besonders authentisieren. Die zugreifbaren Dateien müssen mit einer speziellen Kennzeichnung ("für Wartungszwecke relevant") vom Erzeuger versehen sein, um zugreifbar zu sein (zur Abwehr von B.3). (Hierzu gehören standardmäßig die Dateien HERS Hardware-Error- Recovery-System und SERS Software-Error-Recovery-System).

Schutz von Benutzerdaten in Diagnoseunterlagen

Diagnoseunterlagen bei Systemfehlern werden unter speziellen Benutzerkennungen des Systemverwalters (SYSDUMP und SYSSNAP) abgelegt, so daß sie dem Zugriff durch den normalen Benutzer entzogen sind (zur Abwehr von B.3).

Diagnoseunterlagen von lesegeschützten Auftragsbeschreibungen oder Programmen, die in Situationen anfallen, ohne daß ein Leserecht des Auftrags auf dieses Programm bestand, sondern nur ein Ausführungsrecht, werden ebenfalls unter einer speziellen Benutzerkennung des Systemverwalters (SYSUSER) abgelegt, so daß die Information nur auf Anfrage und in der Regel nur dem Eigentümer der Auftragsbeschreibung oder des Programms zur Verfügung gestellt werden kann. Hierfür stellt das System beschränkten Platz bereit, um bei Mißbrauch eine Beeinträchtigung des Gesamtbetriebs

möglichst gering zu halten. Bei Erschöpfung des Speicherplatzes wegen übermäßiger Beanspruchung können keine Diagnoseunterlagen lesegeschützter Programme mehr erstellt werden. Der Verursacher der Platzbelegung ist ermittelbar (zur Abwehr von B.5, B.6).

Eine Sonderrolle spielen Informationen im Adreßraum eines Benutzerauftrags, die gegen die Übernahme in Diagnoseunterlagen besonders gekennzeichnet sind (sog. Secret-Pages). Bei geeignetem Betriebsmodus werden solche Daten nicht in einen Benutzerdump aufgenommen (zur Abwehr von B.3, B.4).

Der Zugriff über Diagnosetools zu Adreßraumteilen des Systems ist über Testlevel für Lesen und Schreiben geregelt.

Revisionsfähigkeit

- **Revisionsfähigkeit einzelner Aufträge**

Für alle Aufträge werden, gesteuert über Auftragsparameter und Kommandos, Ablaufprotokolle erzeugt, die z.B. alle Kommandos und die durch sie bewirkten Ereignisse enthalten. Bei Bedarf können für Kommandos (die über benutzerkontrollierte Syntaxdateien umbenannt sein können) invariante Standardnamen protokolliert werden.

Benutzern dienen diese Ablaufprotokolle üblicherweise nur für ihre eigene Kontrolle oder um bei vermutetem Fehlverhalten des Systems Unterlagen zu haben. Systemverwaltern und Gruppenverwaltern kann im Rahmen des Auditing des Gesamtbetriebs auferlegt werden, Ablaufprotokolle in geeigneter Ausfürlichkeit zu erstellen und revisionssicher aufzubewahren (zur Abwehr von B.4), um die zentral im Security Audit Trail erfaßten Informationen zu ergänzen. Da solche Ablaufprotokolle üblicherweise sowieso anfallen und als Unterlagen aufgehoben werden, wird dadurch das zentrale Auditing entlastet.

- **Revisionsfähigkeit des Gesamtbetriebs**

Es werden fünf Logdateien geführt, die eine globale Beweissicherung (ggf. unter Einbezug von Ablaufprotokollen einzelner Systemverwalter und Gruppenverwalter) ermöglichen:

- Security Audit Trail (SAT),
- CONSLOG, in dem alle Aktivitäten der Systembedienung aufgezeichnet werden,
- SKP-LOG für SKP-Benutzer und SKP-Startup,
- OMNIS-LOG für Ereignisse von OMNIS-Benutzern,
- DADM-LOG für Netzverwalter-Kommandos.

Die in SAT aufzuzeichnenden Ereignisse werden vom Sicherheitsverantwortlichen (Benutzerkennung SYSPRIV) gesteuert. Der Umfang der in CONSLOG aufgezeichneten Ereignisse ist nicht steuerbar, da diese lückenlos nachvollziehbar sein sollen.

Die aktuelle CONSLOG-Datei wird in SLED-Dumps vermerkt. Ein Logging von Abrechnungsinformation erfolgt in getrennte Dateien. Diese Abtrennung, ebenso wie die weitere Aufspaltung des Loggings sicherheitsrelevanter Information in SAT und CONSLOG dient der Übersichtlichkeit (zur Abwehr von B.6).

Die Auswertung von SAT- und CONSLOG-Dateien erfolgt mit einem gemeinsamen Tool (SATUT), das auch das Zusammenspielen in gemeinsame Dateien erlaubt.

Fehlerüberbrückung und Verfügbarkeit

Die Aufrechterhaltung der Funktionalität des Systems trotz Fehlfunktionen in Hardware und Software, die Gewährleistung der Funktionalität trotz Fehlbedienungen (z.B. provozierte Programmfehler des Benutzers) ist nur partiell möglich und erfordert auch die Mithilfe der Systembedienung und Systemverwaltung. Sie dienen der Abwehr von B.5.

- **Fehlerüberbrückung in Hardware**

Alle Register, Datenwege (Busse), Verarbeitungswerke (z.B.Addierwerk) und der Firmware-Speicher sind bei den zentralen Komponenten paritätsgesichert. In einigen Fällen werden sogar Einzel- oder Doppelfehler über redundante Information behoben.

Auf Plattenspeichern werden bei als defekt erkannten Spuren Ersatzspuren automatisch zugewiesen und unsichtbar für die Systemsoftware, benutzt.

Über auftretende sporadische Fehler werden Fehlerstatistiken geführt, die über den Serviceprozessor gesammelt werden. Durch eine rechtzeitige Präventivwartung (offline oder online, auch über TELESERVICE) kann diese Information abgerufen und dann einem permanenten Ausfall vorgebeugt werden. Darüber hinaus können Peripheriegeräte auch regelmäßig auf ihre Funktionstüchtigkeit (ebenfalls offline oder online) überprüft werden (sog. TDP-Programme und WARTOPT-Funktion). Hierzu muß ggf. nur die Zugänglichkeit des Geräts für die Benutzer unterbunden werden.

- **Fehlerüberbrückung in Software**

Fehlersituationen, die durch Software-Maßnahmen des Betriebssystems gelöst werden müssen, sind zum einen Hardware-Fehler, die zwar von der Hardware erkannt, jedoch nicht behoben werden können. Zum anderen sind dies Software-Fehler in der Logik der Programmläufe des Betriebssystems. Fehler der ersten Art werden - unabhängig, ob korrigierbar oder nicht - von der Hardware durch entsprechende Unterbrechungen gemeldet und in der speziellen Protokolldatei HERSLOG protokolliert. Fehler der zweiten Art werden von der Software, die die Fehlersituationen erkennt, in der Protokolldatei SERSLOG protokolliert.

Die Korrektur (z.B. durch Wiederholung etc.) von Hardwarefehlern erfolgt unabhängig vom Betriebsmodus des aktuell betroffenen Benutzerprogramms. Bei permanenten Fehlern, die als nicht behebbar erkannt worden sind, wird versucht, erneute Fehler zu verhindern, indem bei redundant konfigurierten Hardware-Bausteinen diese aus der Konfiguration entfernt werden. Dies kann periphere Geräte, Kanäle, Ein-Ausgabeprozessoren und Zentralprozessoren betreffen. Über die Nutzung des Dual-Recording-by-Volume (DRV) werden speziell Plattenausfälle überbrückt.

Als Softwarefehler erkannte Fehlersituationen werden standardmäßig der direkt auftraggebenden Softwareinstanz (entweder eine Funktionseinheit des Systems oder ein Benutzerprogramm) zurückgemeldet, in schweren Fällen wird entweder der Programmlauf des Benutzers abgebrochen oder sogar der Auftrag (Job) des Benutzers beendet. Dabei wird entsprechende Diagnoseinformation - Benutzerdump oder Systemdump - erzeugt.

In beiden Fällen ist der verursachte Schaden relativ begrenzt. Der Programmlauf oder der Auftrag kann wiederholt werden. Soweit Betriebsmittel von der Fehlersituation nicht betroffen sind, stehen diese dann erneut zur Bearbeitung zur Verfügung.

Fehler, die die Funktionsfähigkeit des Gesamtsystems betreffen, lösen eine abnormale Systembeendigung (CRASH) aus. Hierbei werden die Daten des Systems und der Benutzer eingefroren, um sie mit Diagnosefunktionen sicherstellen und auswerten zu können. Über ein Kommando des Operateurs kann das automatische Sicherstellen ohne manuelle Eingriffe veranlaßt werden. Die Ursachenanalyse für die Fehlersituationen wichtiger Funktionseinheiten im BS2000 wird durch permanent mitlaufende bzw. einschaltbare Traces unterstützt.

- **Gewährleistung der Funktionalität**

Eine Gewährleistung der Funktionalität bei Hardware- und Softwarefehlern erfordert z.T. die Mithilfe des Operateurs. Fehlersituationen, die nicht vom System selbst behandelt werden können, werden dem Operateur gemeldet (z.B. "Leistungsabfall"). Auch aus anderen ihm vom System ausgegebenen Informationen kann der Operateur auf den Defekt einzelner Hardware- oder Softwarekomponenten schließen. Dem Operateur wird dazu die Möglichkeit gegeben, von sich aus die Hardware- oder Softwarekonfiguration des Systems zu verändern, insbesondere Hardware-Komponenten zu-

und wegzuschalten oder einzelne Subsysteme (soweit hierfür die Voraussetzung gegeben ist) neu zu starten oder sogar auszuwechseln. Dies betrifft bei Mehrprozessoranlagen einzelne Zentralprozessoren, Ein-/Ausgabeprozessoren, Kanäle und periphere Geräte. Das System sorgt bei Prozessoren und Pfaden dafür, daß dabei, soweit möglich, keine Information verloren geht, bei speichernden Komponenten dafür, daß die gespeicherte Information, soweit möglich, konsistent bleibt.

Durch Wegschalten von Hardware-Komponenten oder Pfaden zu diesen darf die prinzipielle Funktionsfähigkeit des Systems nicht beeinträchtigt werden. Daher werden Aufträge zum Wegschalten einer wichtigen Komponente (letzter Ein-/Ausgabeprozessor, letzte Konsole, letzte Pfad zu einem Gerät) zurückgewiesen.

Wegschalten von Prozessoren führt zur Verringerung der Leistungsfähigkeit. Durch die prioritäts- und zeitscheibengesteuerte Prozessorvergabe wird sichergestellt, daß

- Systemprozesse nicht durch Benutzerprozesse dominiert werden können,
- Benutzerprozesse auch in Engpaßsituation entsprechend der ihnen zugewiesenen relativen Prioritäten bearbeitet werden.

Maßnahmen gegen Datenverlust

Jeder Benutzer kann alle Daten (Dateien, Jobvariable), die unter seiner Benutzerkennung abgelegt sind, auf Hintergrunddatenträger, i.a. Bänder, sichern, wobei er Umfang und Art der Sicherung wählen (Dateiauswahl, Deltatechnik etc.) und die Daten bei Bedarf wieder einspielen kann. Die Benutzerkennung TSOS hat, da sie für alle Datenobjekte Ersatzeigentümer ist, die Möglichkeit, Datensicherung und Wiederherstellung übergreifend zu allen Benutzerkennungen durchzuführen.

Betrieb und Bedienung

Die Betriebsüberwachung und Steuerung erfolgt über Benutzerkennungen, denen Systemverwaltungsprivilegien zugewiesen worden sind. Die Bedienung erfolgt über als Bedienungskonsolen ausgezeichnete Terminals oder über (sog. privilegierte) Anwendungen, die als Stapelaufträge laufen, als Dialogaufträge über Terminals bedient werden, oder einen eigenständigen Terminalbetrieb organisieren (z.B. Subsystem OMNIS). Beides erfolgt durch speziell ausgewähltes Personal, dessen Tätigkeiten speziell organisiert (z.B. Aufgabentrennung, Einbindung in feste Verfahren) und überwacht werden kann (zur Abwehr von B.2, B.4, B.7). Die Systembedienung kann durch ausschließliche Nutzung von privilegierten Anwendungen automatisiert werden. Man spricht dann von bedienerlosem Betrieb.

Sicherheitsaufgaben der Systemverwaltung

Die Sicherheitsaufgaben der Systemverwaltung umfassen

- Vergabe von Systemverwalterrechten nur durch die Benutzerkennung SYSPRIV des Sicherheitsbeauftragten,
- Benutzerverwaltung (mehrstufig aufteilbar),
- Audit-Auswertung,
- Datenpflege,
- Systemgenerierung und Installierung,
- Hardware- und Software-Wartung.

Hierfür sind folgende Rollen vorgesehen:

- der Sicherheitsbeauftragte,
- der Benutzerverwalter,
- der Audit-Auswerter,
- ggf. verschiedene Systemverwalterrollen.

Die Rolle des Sicherheitsbeauftragten ist fest einer Benutzerkennung zugeordnet und ist mit allen anderen Rollen unvereinbar. Ihr obliegt neben der Vergabe von Systemverwalterrechten auch das Schalten des Sicherheits-Audits.

Die Rolle der Benutzerverwaltung ist weitgehend freizügig an Benutzerkennungen zu vergeben. Sie ist in sich wieder unterteilt in Unterrollen.

Die Rolle der Audit-Auswertung ist an mehrere Benutzerkennungen vergebbar, standardmäßig aber immer zu einer ausgezeichneten Benutzerkennung (SYSAUDIT) zugeordnet.

Die übrigen Systemverwalterrollen können unter Ausnutzung der gebotenen Privilegierungsmechanismen, verschieden definiert und gegeneinander abgegrenzt werden.

Privilegienvergabe

Über die Vergabe von Systemprivilegien wird Benutzerkennungen die Wahrnehmung von Aufgaben der Systemverwaltung ermöglicht, auch wenn sie nicht zu den ausgezeichneten Benutzerkennungen TSOS und SYSPRIV gehört. TSOS sind standardmäßig alle Systemverwalterrechte zugeordnet bis auf

- Systemverwalterrechte an Benutzerkennungen zu vergeben und ihnen zu entziehen,
- Audit-Dateien auswerten zu dürfen,
- OMNIS-Verwaltungsfunktionen auszuführen,
- Hardware-Wartungsfunktionen anzustoßen.

WeiteresSystemverwalterrecht, das delegiert werden kann:

- Verwaltung des Bandkatalogs (Subsystem MAREN).

Systemverwalterrechte zu vergeben, ist der ausgezeichneten Benutzerkennung SYSPRIV vorbehalten, wobei SYSPRIV keine Rechte an sich selbst vergeben darf (zur Abwehr von B.4). SYSPRIV ist damit für die Aufgaben- und Gewaltenteilung der Systemverwaltung allein verantwortlich. Zur tatsächlichen Etablierung von Benutzerkennungen mit PUBSET-Nutzungsrechten, Benutzerrechten und verfügbarem Kommandosatz sind allerdings Zulieferungen insbesondere von der Benutzerverwaltung nötig. Auch die Zuordnung zu natürlichen Personen, ein wesentlicher Aspekt bei der Durchsetzung einer Rollenseparierung, ist Aufgabe der Benutzerverwaltung.

Die OMNIS-Verwaltungsfunktion ist über eine netzweit wirkende, von den Benutzerkennungen einer einzelnen Anlage unabhängige Authentisierung mittels Paßwörter zugänglich.

Die Hardware-Wartungsfunktion ist an die ausgezeichnete Benutzerkennung SERVICE gebunden.

Benutzerverwaltung

¨ **Globale und gruppenspezifische Benutzerverwaltung**

Die Benutzerverwaltung teilt sich in zwei prinzipielle Teilbereiche auf:

- Globale Benutzerverwaltung (über ein entsprechendes Privileg (USERADM) etabliert), und
- gruppenspezifische Benutzerverwaltung (als Gruppenverwalter ausgezeichnete Benutzerkennung in einer Benutzergruppe etabliert).

Der erste Teilbereich ist dem zweitem übergeordnet. Gruppen der obersten Stufe können nur von der globalen Benutzerverwaltung und vom optionalen Gruppenverwalter der Gruppe *UNIVERSAL erzeugt und gelöscht werden. Die gruppenspezifische Benutzerverwaltung kann ersatzweise durch den Gruppenverwalter einer übergeordneten Gruppe oder durch die globale Benutzerverwaltung wahrgenommen werden.

Die Verantwortung für die Benutzerverwaltung ist also hierarchisch, wobei an der Spitze der Hierarchie die Verantwortung für die globale Benutzerverwaltung von mehreren Benutzerkennungen getragen werden kann.

Die Benutzerverwaltung ist nicht nur für die maßgeschneiderte Ausstattung aller Benutzer mit Einzelrechten, PUBSET-Nutzungsrechten und verfügbarem Kommandosatz verantwortlich, sondern auch für die Regelung der Benutzer-Authentisierung und der Nutzung von Zugangsklassen.

Die Gruppenstruktur (hierarchische Baumstruktur) ermöglicht eine Dezentralisierung der Verwaltung von Benutzerkennungen und erleichtert dadurch bei großen Installationen, Benutzer in überschaubaren Einheiten zu verwalten (zur Abwehr von B.6).

- **Wechselspiel zwischen Benutzerverwaltung und übriger Systemverwaltung**

Die Benutzerverwaltung, die personell von anderen Systemverwaltungstätigkeiten trennbar ist, ist teilweise von Zulieferungen der anderen abhängig, teilweise liefert sie ihnen zu.

Die detaillierte Ausprägung des einer Benutzerkennung verfügbaren Kommandosatzes wird von der Systemverwaltung mit gesonderten Kommandos festgelegt. Die Zulieferung erfolgt zu einer abgesprochenen "Profile-id", die bei der Benutzerkennung eingetragen ist.

Das Konzept eines Kommandoprofils beruht auf der Annahme, daß üblicherweise die Verwaltung von Benutzergruppen und von Syntaxdateien durch verschiedene Personen erfolgt. Beschäftigt sich der Gruppenverwalter neben der Zuordnung von Betriebsmittelkontingenten und Einzelrechten mit der Zuordnung des Kommandoprofils zu Benutzerkennungen, so beschäftigt sich eine andere Instanz mit der Pflege der Syntaxdateien, die im Zuge von Änderungen der Software-Konfiguration, des Wartungsstandes (Fehlerkorrekturen) oder funktioneller Änderungen in einzelnen Kommandoprofilen notwendig wird.

Beide Tätigkeiten, sowohl die Verwaltung von Benutzerkennungen, als auch die Pflege von Syntaxdateien haben ggf. ein großes Änderungsaufkommen. Die Kommandoprofile beschreiben eine zwischen beiden Tätigkeiten stabile Zwischenschicht, da sie die grundsätzliche Arbeitsteilung in einer Installation widerspiegelt und deshalb nur geringen Änderungen unterworfen ist. Im Falle von Änderungen werden von seiten des Gruppenverwalters die Anforderungen bzgl. Einführung neuer Kommandoprofile oder Änderung bestehender an den Verwalter von Kommandoprofilen gestellt. Die Zuweisung zu Benutzerkennungen erfolgt durch den Gruppenverwalter. Diese Rollentrennung dient zur Abwehr von B.4 in Kombination mit B.6.

Die Benutzerverwaltung muß auch die Vorleistungen bringen für Tätigkeiten der Systemverwaltung wie die Performance- und Ablaufsteuerung (z.B. die Festlegungen über Abrechnungsdaten: Account-Kennzeichen, verbrauchbare CPU-Zeit, etc.) und Platzbelegungen (PUBLIC-SPACE-LIMIT, RESIDENT-PAGES, CSTMP-MACRO-ALLOWED). Für Sonderrechte bzgl. der Ablaufsteuerung (NO-CPU-LIMIT, START-IMMEDIATE) gilt, daß dieses Sonderrecht wahlweise auch durch eine bei der Ablaufsteuerung (Subsystem JMS, Dienstprogramm JMU) erfolgte Zuweisung erworben werden kann.

Audit-Auswertung

Die Audit-Auswertung wird als Systemverwalterrecht vergeben und ist der standardmäßig vorgesehenen Benutzerkennung SYSAUDIT immer zugewiesen. Dieser Benutzerkennung gehören die Dateien des System-Audit-Trail, ohne daß ein Änderungsrecht auf diese Dateien besteht. Auch die CONSLOG-Dateien ebenso wie die SAVEREP-Dateien sind unter dieser Benutzerkennung abgelegt.

Datenpflege

Der Datenpflege unterliegen alle Aufgaben der Archivverwaltung bzgl. Datenträger, der halbautomatisierten Datenmigration und des Schlüsseldienstes in Bezug auf verlorene oder auszutauschende Paßwörter.

Zur Einschränkung der Mißbrauchsmöglichkeiten sollten diese Tätigkeiten in feste Verfahren eingebettet sein, die Benutzern nicht erlauben, beliebige Programme zu starten.

Systemgenerierung und Installierung

Hierunter fällt die Möglichkeit, ein neues BS2000-System zu generieren, wobei die zum Ablauf kommende Systemsoftware festgelegt wird.

Die Festlegung umfaßt hierfür drei Teile:

- das Ladesystem, das zum Generierungszeitpunkt vorgebunden wird, so daß einzelne Teile nicht mehr ausgetauscht werden können, und das die Generierungsoptionen enthält;
- eine Menge nachgeladener Systemteile, die über im Ladesystem festgelegte Namen angesprochen werden;
- eine Menge von automatisch (bei Installierung) oder bei Bedarf nachzuladender Subsysteme, die über den Subsystemkatalog verankert werden, wobei dieser noch zur Laufzeit des Systems verändert werden kann.

Die beim Ladevorgang zur Anwendung kommenden Korrekturdateien (Repfiles) werden per Namen festgelegt.

Die Hardware-Konfiguration der Peripherie bei CFCS3 wird aus einer Datei in den Serviceprozessor für einen nachfolgenden Ladevorgang hinterlegt.

Die zum Einsatz benötigten Syntax-Dateien und Meldungs-Dateien für das System und für die einzelnen Profile-ids können von vorangehenden Systemläufen des F2/Q3-Systems übernommen werden, wobei ein Bezug über Startup-Parameter-Options hergestellt werden kann.

Die Generierung des Datenfernverarbeitungssystems erfolgt unabhängig von der Generierung des BS2000-Systems. Die Kopplung der beiden Systeme erfolgt über den Anschluß der PDN-Rechner ans BS2000.

Die Initialisierung von Datenträgern, insbesondere von Plattendatenträgern, die dann z.B. zur Installierung eines Systems benötigt werden, ist Teil der Generierung eines Systems. Da hiermit auf diesem Datenträger hinterlegte Schutzinformation überschrieben wird, ist diese Tätigkeit, wie die gesamte Generierung und Installation, nur unter besonderer Kontrolle und von vertrauenswürdigem Personal auszuführen.

Vor der Installierung eines Systems oder einzelner Komponenten wie Syntax-Dateien sollte das Ergebnis einer Generierung einem Review unterzogen werden, um z.B. das Einbringen von als unsicher bekannten Subsystemen oder gar von Trojanischen Pferden in das System zu erschweren. Eine mögliche Maßnahme ist die Rückverfolgung der Bestandteile des montierten Systems (und deren Modifikationen). Hierbei ist insbesondere zu beachten, daß es bei Einsatz von betreiberspezifischen Systemergänzungen (als System-Exits geladene Subsysteme) zu Verfälschungen der vom System erfolgten Sicherheitsleistung kommen kann. In der zertifizierten Version BS2000-SC V10.0 sind System-Exits nicht zulässig.

Die Nachvollziehbarkeit aller Vorgänge des Systemstarts ist durch eine vollständige Protokollierung aller Interaktionen des Operateurs mit dem System einschließlich auch der mittelbar wirksam werdenden Systemparameter in CONSLOG gegeben. Diese wird ergänzt durch die ebenfalls lückenlose Protokollierung aller ins System eingespielten Korrekturen (Ladesystem, Subsysteme, nachgebundene Bindemodule).

Hardware und Software-Wartung

Hierunter fällt

1. Online-Hardware-Diagnose (Ablauf spezieller Prüfprogramme)
2. Hardware-Diagnose-Auswertung
3. Online-Software-Diagnose (Einsatz spezieller Tools)
4. Software-Diagnose-Auswertung

5. Nutzung spezieller Testprivilegierungen.

Bei geeigneter Auswahl der Verfahren sind bei 1. und 2. die geringsten Möglichkeiten der unerwünschten Informationsgewinnung oder der Betriebsstörung gegeben (Subsystem WARTOPT).

Bei 3., 4. und 5. besteht dagegen grundsätzlich die Möglichkeit, daß beliebige Information gewonnen werden kann. Einschränkungen sind hier durch bei der Generierung zu setzende Systemparameter, durch von der Benutzerverwaltung festzulegende Testprivilegien sowie durch die Nutzung von Secret Pages möglich. (Subsystem AIDSYS).

Es ist einerseits Aufgabe der Benutzerverwaltung, hier nur vertrauenswürdiges Personal zuzulassen, andererseits die Tätigkeitszeiträume so einzuschränken und dies im Rahmen der Performance- und Ablaufsteuerung sicherzustellen, daß keine Kollision mit sicherheitsrelevanten Abläufen im System stattfindet.

Sicherheitsaufgaben der Systembedienung

- **Einbindung**

Die Systembedienung hat spezifische Aufgaben, die allein ihr vorbehalten sind, wie die Systemeinleitung oder die Bedienung peripherer Geräte, aber auch Aufgaben, die sich mit der Systemverwaltung überlappen oder als sogenannte "Spezialkommandos" von der Systemverwaltung an die Systembedienung übertragen worden sind.

Die Übertragung von Spezialkommandos an den Operateur (zusätzlich zu den ihm standardmäßig zur Verfügung stehenden Normalkommandos) erfolgt zum Zeitpunkt der Systemgenerierung.

Die Kontrolle der Systembedienung obliegt der Systemverwaltung und erfolgt in erster Linie durch Auswertung der ausführlichen Aktivitätenaufzeichnung (Medium CONSLOG und Blattschreiberprotokoll) im Nachhinein. Es ist natürlich auch eine direkte Überwachung im laufenden Betrieb möglich, u.a. dadurch, daß ein Systemverwalter als Teilnehmer die Betriebssituation verfolgt.

- **Zugangsschutz**

Der Zugangsschutz für das Hochfahren des Systems ist durch den physikalischen Schutz der Hauptkonsole gegeben. Im laufenden Betrieb kann über geeignete Vorgaben (SKP, OMNIS-Einsatz) auch ein personenbezogenes Logging von mehreren Operateuren erreicht werden, die parallel und nicht notwendigerweise an physikalisch geschützten Konsolen oder Terminals arbeiten.

- **Systeminstallierung und -überwachung**

Dem Operateur obliegt der Systemstart (STARTUP) einschließlich des Startens des Datenkommunikationssystems. Hierbei sind die Vorgaben der Systemverwaltung zu beachten, damit das System auf einer korrekten Hardwarekonfiguration zum Ablauf gebracht wird. Bei Betriebssituationen, die schwerwiegende Fehlersituationen vermuten lassen, kann der Operateur Diagnoseunterlagen erzeugen lassen und ggf. den Systemlauf beenden. (Diagnoseunterlagen werden allerdings auch vom System selbst erzeugt.) Die physikalische Sicherung von dabei anfallenden Datenträgern obliegt dem Operateur.

Der Operateur kann Einfluß auf die Softwarekonfiguration im laufenden Betrieb nehmen, in dem gezielt Subsysteme gestartet und beendet werden.

Bei Programmen, die von Systemverwaltern zum Ablauf gebracht werden und privilegiert ablaufende Teile enthalten, wird der Operateur involviert.

- **Bedienung peripherer Geräte**

Dem Operateur obliegt nicht nur der physische Schutz von Datenträgern, sondern auch die korrekte Behandlung von Datenträgeranforderungen - dies in Übereinstimmung mit von der Benutzerverwaltung vergebenen Rechte an einzelne Benutzer. Dies spielt insbesondere beim Import von Datenträgern, die von fremden Anlagen stammen, eine wichtige Rolle.

Die Veränderung der Gerätekonfiguration (Schalten von Wegen; Zuschalten neuer, Abschalten defekter Geräte) ist ebenfalls Aufgabe des Operateurs.

2.1.3 Regelvorgaben durch und für den Benutzer

2.1.3.1 Benutzerkennungen

Zuordnung zu natürlichen Personen

Benutzerkennungen repräsentieren natürliche Personen. Natürliche Personen benötigen eine Benutzerkennung, als deren legaler Eigentümer sie sich authentisieren müssen, um mit dem System zu arbeiten, zur Abwehr von B.1.

(1) Eine Person kann für verschiedene Aufgaben mehrere, verschiedene Benutzerkennungen benutzen, wird dann aber durch das BS2000 so bedient, als würde es sich um getrennte Personen handeln.

(2) Umgekehrt können mehrere Personen gemeinsam eine Benutzerkennung benutzen, werden dann aber durch das BS2000 bzgl. der Abwicklung oder der Abrechnung ihrer Tätigkeiten nicht voneinander unterschieden.

Dies heißt nicht, daß für eine Benutzerkennung nur ein Auftrag (Dialog, Stapel) ausgeführt wird. Das BS2000 unterstützt hier beliebige Parallelarbeit. Insbesondere können mit Hilfe des Subsystem OMNIS auch von einem Datensichtgerät aus mehrere Dialoge parallel geführt werden.

Diese Flexibilität der Zuordnung von Person zu Benutzerkennung erlaubt mehrere Anwendungsfälle. Typisches Beispiel für (1) ist, daß ein Systemverwalter für Standardtätigkeiten wie das Schreiben eines Briefes, wo besondere Privilegien nicht erforderlich sind, sich einer unprivilegierten Benutzerkennung bedient. Beispiel für (2) ist, daß der Vertreter einer Person deren Aufgaben erledigen kann, ohne jedes einzelne Privileg oder Recht der zu vertretenden Person gesondert übertragen bekommen zu müssen.

Für Revisionszwecke (zur Abwehr von B.4) ist allerdings bei Chip-Karten-Nutzung die Voraussetzung gegegeben, daß eine personenbezogene Protokollierung der von einer Person angestoßenen Tätigkeiten erfolgen kann.

Das personenbezogene Logging dient im Fall (1) dazu, daß übergreifend über einzelne Benutzerkennungen die von einer Person angestoßenen Tätigkeiten rückverfolgt werden können. Im Fall (2) dient es dazu, zwischen den einzelnen Personen bei der Rückverfolgung ihrer Verantwortlichkeit unterscheiden zu können.

Faßt man die Benutzerkennung als den juristischen Vertragspartner des Betreibers einer BS2000-Anlage auf, so heißt dies, daß eine Person mehrere Verträge abschließen kann (1), und daß ein einzelner Vertrag mit mehreren Personen geschlossen werden kann (2). Dies ermöglicht die Freiheit, Benutzerkennungen projektbezogen und aufgabenbezogen einzurichten. Bietet das personenbezogene Logging bei (1) dem BS2000-Betreiber eine weitergehende Möglichkeit, Sicherheitsverletzung zu erkennen, so bietet es bei (2) dem Vertragspartner die Möglichkeit, die Verantwortlichkeit intern weiterzuverfolgen.

Die geschilderte Flexibilität entspricht den in der Praxis angetroffenen Verhältnissen und Arbeitsweisen. Eine strikte 1:1-Zuordnung von Person zu Benutzerkennung ist eine in der Praxis immer nur annäherungsweise durchsetzbare Einschränkung.

Nutzung von Benutzerkennungen

Um den Zugang unberechtigter Personen zum System zu verhindern (zur Abwehr von B.1) wird eine dem Zugangsweg spezifische Authentisierung vorgesehen. Dies soll insbesondere verhindern, daß die Zugangshürden aus Bequemlichkeitsgründen (häufige Nutzung nur von vertrauenswürdiger Seite) zu niedrig gesetzt werden, oder daß die Authentisierungsinformation zu weit gestreut werden muß (zur

Abwehr von B.6). Authentisierungsanforderung und Einschränkungen der Zugangswege sind deshalb weitgehend getrennt regelbar. Die zur Authentisierung benötigten Daten werden der SRPM-Datei des als sogenannten Home-PVS angeschlossenen Public Volume Sets entnommen.

BS2000 unterscheidet mehrere Zugangsklassen:

1. Dialog-LOGON (zur Erzeugung eines Dialog-Auftrags)
2. Stapel-LOGON (zur Erzeugung eines Stapel-Auftrags) z.B. von einem anderen Benutzerauftrag aus
3. Remote-Batch-Logon (in einem F2/Q3-System nicht in der Softwarekonfiguration vorgesehen).

Jede Zugangsklasse kann durch die Systemverwaltung pro Benutzerkennung getrennt gesperrt werden, darüber hinaus kann sie durch spezifische Authentisierungsvorgaben für die berechtigten Personen und durch spezifische Zugangseinschränkungen weitgehend getrennt geschützt werden:

	Authentisierung	Zugangseinschränkung
Bei 1:	Paßwort *1, Chipkarte (einzeln, gemeinsam oder keines erforderlich)	Datensichtgeräte (über Anschlußadresse identifiziert) Jobklassensperrung
Bei 2:	Paßwort *1 oder keine Authentisierung	Absetzende Benutzerkennung Jobklassensperrung *2
Bei 3:	Paßwort *1 oder keine Authentisierung	Jobklassensperrung *2

Mit *1 und *2 wird angezeigt, daß der Wert der entsprechenden Steuergröße für die betroffenen Zugangsklassen nur gemeinsam gesetzt werden kann.

Es ist z.B. möglich, für Dialog-Logon die Chipkarte zu verlangen, für den Stapel-Logon nur Zutritt von vorgegebenen (vertrauenswürdigen) Benutzerkennungen zu erlauben und den Zugang über Remote-Batch-Logon gänzlich zu verbieten.

Für das Paßwort einer Benutzerkennung kann eine Vorgabe bzgl. seiner Gültigkeit für den Zugang gemacht werden. Es ist dann Aufgabe des Benutzers, dieses häufig genug zu ändern. Zusätzlich kann die Lebensdauer eines Paßworts einer Benutzerkennung begrenzt werden.

Die getrennte Schützbarkeit der Zugangsklassen (zur Abwehr von B.1 und B.6) dient z.B. folgenden Zwecken:

- Sperren des Zugangs zu hochprivilegierten Benutzerkennungen
- Einschränken des Zugangs auf besonders geschützte Zugangswege (z.B. für spezielle, physikalisch vom Betreiber geschützte Datensichtgeräte)
- Einschränken des Zugangs auf die Authentisierung mittels Chipkarte (z.B. Stapel-Zugang ist dann nur von der eigenen Benutzerkennung möglich)

Rechte und Eigenschaften einer Benutzerkennung

Für eine Benutzerkennung ist neben den Attributen, die das Vertragsverhältnis zwischen Anlagenbetreiber und Benutzer beschreiben, wie Postadresse, Abrechnungsnummern, Betriebsmittelverbrauch, verwaltungstechnische Gruppenzugehörigkeit und neben den Zugriffsdefinitionen festgelegt, welche

Dateien dem Benutzer gehören (zur Abwehr von B.3) und welche Rechte (zur Abwehr von B.2) ihm zugeteilt worden sind bzgl.

- system-globalen Rechten
- Benutzerrechten,
- PUBSET-Nutzungsrechten,
- verfügbarem Kommandosatz.

Die Vergabe dieser Rechte erfolgt durch die System- bzw. Benutzerverwaltung

Eigentümerschaft von Dateien und Jobvariablen

Die einer Benutzerkennung zugeordneten Dateien und Jobvariablen bilden einen Teilbaum im Dateikatalog bzw.im Jobvariablenkatalog eines PUBSET (Public Volume Set). Das Eigentümerrecht bezieht sich auf das Erzeugen und Löschen von Objekten in diesem Teilbaum (die auch zu Lasten des Benutzers abgerechnet werden), das Festsetzen der Zugriffsrechte für andere Benutzer und von Objektattributen. Dateien und Jobvariable können dabei ausschließlich der Nutzung durch den Eigentümer selbst vorbehalten werden - das ist der Standardfall.

Die Eigentümerschaft an einer Datei oder Jobvariablen ist fest an die Benutzerkennung geknüpft, unter der die Datei oder Jobvariable bei der Erzeugung katalogisiert wurde, und kann nicht übertragen oder geändert werden.

Die Dateien und Jobvariablen einer Benutzerkennung sind benennungsmäßig und, wenn Benutzerkennungen aufgabenbezogen eingerichtet werden, auch entsprechend aufgabenmäßig gruppiert. Dies erleichtert die Festlegung der Zugriffsrechte anderer Benutzer auf sie.

Die System-globalen Rechte werden zur Erledigung von Teilaufgaben der Systemverwaltung benötigt und gelten Pubset-übergreifend für das ganze System.

Bei den Benutzerrechten, also Rechten, die nicht Systemverwalterrechte sind, spielt das Gruppenverwalterrecht eine besondere Rolle. Die Benutzerkennungen im BS2000 können hierarchisch, pro PVS unabhängig voneinander, in Gruppen organisiert werden.

Neben dem organisatorischen Aspekt von Benutzergruppen durch verschiedene Gruppenverwalter können Nutzungsrechte an Betriebsmitteln über die Zuordnung von Benutzern zu Benutzergruppen abgestuft vergeben werden (dient damit auch zur Abwehr von B.3). Die Gruppenzugehörigkeit eines Benutzers ist hierbei immer durch die Gruppenstruktur des Home-Pubsets gegeben.

Neben dem Gruppenverwalterrecht gibt es noch das Recht, Bandkennsätze zu ignorieren, das Recht zur Nutzung von Abrechnungskennzeichen (Accounts), die Möglichkeit, Teile von Adreßräumen resident zu setzen (CSTMP-Makro), Programme mit speziellen Speicherschlüsseln zu laden, Testprivilegien zu setzen, Aufträge unter speziellen Abrechnungskennzeichen als Express-Läufe, ohne Zeitbeschränkung oder nicht deaktivierbar zu starten sowie andere, wie z.B. für Dateien ein Audit-Bit zu setzen.

Es gelten jeweils die Einzelrechte, die auf dem Home-Pubset - auf dem auch die LOGON-Validierung durchgeführt wurde - eingetragen sind. Ein Benutzerrecht bezieht sich entweder auf einzelne Objektklassen oder auf das System als Ganzes.

PUBSET-Nutzungsrechte

Nur *die* Benutzer können auf einem Pubset arbeiten, die einen Benutzereintrag im Benutzerkatalog dieses Pubsets haben.

Verfügbarer Kommandosatz

Jeder Benutzerkennung kann der Name eines Kommandoprofils (Profile-Id) zugeordnet werden. Das Kommandoprofil definiert den zulässigen Kommandosatz, der für diese Benutzerkennung verfügbar ist.

Die von einem Benutzer ausführbaren Kommandos (einschl. von Programmanweisungen) werden dabei über bis zu drei Syntaxdateien, die die vollständigen Syntaxdefinitionen der eingebbaren Kommandos enthalten, interpretiert. Diese spielen bei der Analyse eines eingegebenen Kommandos zusammen:

1. Benutzer-kontrollierte Syntaxdatei (für Umbenennungen und Steueranweisungen von Programmen unter Kontrolle des Benutzers)
2. Gruppenverwalter-kontrollierte Syntaxdatei (für spezifische Einschränkungen und Ergänzungen, die über das Kommandoprofil adressiert werden
3. Systemverwalter-kontrollierte Syntaxdatei.

Diese Aufteilung dient folgenden Zwecken: Über 3. können die in einem System über Kommandos zugänglichen Funktionen generell modifiziert und eingeschränkt werden. Über 2. kann dies vom Gruppenverwalter bzgl. einzelner Benutzer unabhängig erfolgen. 1. erlaubt, daß der Benutzer weitere Modifikationen vollständig unter seiner Kontrolle machen kann, ohne die unter 2. und 3. getroffenen Vorgaben zu gefährden (Abwehr von B.2 und B.6).

Ein wichtiges Beispiel für die Einschränkbarkeit eines einzelnen Benutzers ist, daß nur einige vorgegebene Programme durch spezifische Kommandos aufrufbar sind. Dies dient neben der Abwehr von B.3 insbesondere der Abwehr von B.4, da Privilegien einem Benutzer streng gekoppelt an ein spezielles Verfahren gewährt werden können. Eine freie Nutzung, bei der Fahrlässigkeit oder Mißbrauch möglich ist, kann dabei vermieden und ausgeschlossen werden. (Die freie Wahl des Programms kann durch die Sperrung des Kommandos START-PROGRAM - bzw. auch LOAD-PROGRAM, EXEC, LOAD - verhindert werden. Eine andere Möglichkeit ist, Programme nur über Prozeduren und Prozeduren nur über die in der durch den Gruppenverwalter kontrollierten Syntaxdatei definierten Kommandos aufrufbar zu machen. Hierbei können noch spezifische, nur über Kommandos mögliche Einstellungen für ein Programm in unverfälschbarer Weise erzwungen werden.) Andere formulierbare Einschränkungen betreffen die Zugänglichkeit von Operanden und den Wertebereich von Operandenwerten. Einschränkungen dieser Art sind besonders bei Benutzerkennungen mit hoher Privilegierung sinnvoll, um den möglichen Mißbrauch zu beschränken.

Rechte und Eigenschaften von Benutzeraufträgen

Benutzeraufträge werden in Form von Auftragsbeschreibungen an das System gestellt. Bei Dialog-Aufträgen besteht eine Auftragsbeschreibung nur aus dem LOGON-Kommando, bei Stapel-Aufträgen aus einer Datei, die mit einem LOGON-Kommando eingeleitet wird (dessen Parameter nicht ausgewertet werden), und Parametervorgaben, die dem Operanden in einem LOGON-Kommando entsprechen.

Mit Beginn der Bearbeitung wird jedem Benutzerauftrag ein Taskprozeß zugeordnet, der die Rechte und Privilegien der Benutzerkennung, die im LOGON adressiert worden ist, übernimmt. Zusätzliche Rechte auf ablaufspezifische Objekte werden dem Taskprozeß für die Abarbeitung des einzelnen Auftrags zugewiesen.

Es können zu einem Zeitpunkt mehrere Benutzeraufträge mit der gleichen Benutzerkennung laufen. (Einschränkungen sind hier bzgl. Zugangsklassen mittelbar über die Zuordnung zu Jobklassen, die der Performanceoptimierung dienen, möglich.) Jeder dieser Taskprozesse hat dann gleiche Privilegien und Rechte auf den Betriebsmitteln der Benutzerkennung, aber verschiedene Rechte bezüglich der Betriebsmittel, die spezifisch für oder durch den einzelnen Taskprozeß erzeugt werden.

Laufende Aufträge und Auftragsbeschreibungen noch nicht gestarteter Aufträge sind von allen Aufträgen derselben Benutzerkennung aus sichtbar (über Informationsdienste) und können von ihnen auch abgebrochen werden.

Kooperation über und mehrfache Nutzung von Betriebsmitteln kann unabhängig davon organisiert werden, ob diese der Benutzerkennung oder dem Taskprozeß gehören. Für Aufträge der gleichen Benutzerkennung wird die Organisation von Kooperation besonders unterstützt.

1. Abbrechen eines anderen Auftrags (z.B. um eine Bearbeitung in Schleife zu unterbrechen) oder eines anderen Ausgabeauftrags (SPOOL-Job) ist nur für Aufträge der gleichen Benutzerkennung möglich.
2. Zugriff auf Betriebsmittel der Benutzerkennung sind möglich:
   - bei Benutzerschaltern: Schreiben nur für Aufträge der gleichen Benutzerkennung
   - bei Dateien, Jobvariablen und Bändern soweit durch Schutzattribute gestattet
3. Zugriff auf Betriebsmittel des Taskprozesses sind möglich:
   - Memory-Pools, soweit für Taskprozesse derselben Benutzerkennung, derselben Benutzergruppe oder für alle Benutzerkennungen freigegeben
   - Event-/Serialisations-Items (siehe Memory-Pools)
   - DCAM-Anwendungsnamen/Verbindungsnamen, soweit Name und Paßwort bekannt

Darüber hinaus gibt es Betriebsmittel, die dem Taskprozeß allein vorbehalten sind:

- Auftragsschalter;
- Teile des Benutzeradreßraums, die nicht in Memory-Pools mit Scope ungleich "local" liegen;
- temporäre Dateien.

2.1.3.2 Objektschutz

Festlegung der Schutzattribute

Der Objektschutz wird durch den Eigentümer oder den Erzeuger eines Objektes geregelt und dient der Abwehr von B.3. Dateien, Jobvariable und Bänder sind einer Benutzerkennung als Eigentümer zugeordnet. Nur Aufträge dieser Benutzerkennung oder ein entsprechend privilegierter Systemverwalter können diese Objekte erzeugen und löschen und deren Attribute ändern, insbesondere können nur sie die Zugriffsrechte für andere Benutzerkennungen festlegen und ändern.

Zugriffsrechte können getrennt für die einzelnen Zugriffsmodi festgelegt werden:

- Bei katalogisierten Dateien, über Paßwörter und wahlweise über
  * Standardschutzattribute (Schreibverbot, Fremdzugriffsverbot),
  * Basic-ACL, die nach Benutzerkennung des Datei-Eigentümers, Benutzergruppe und übrige Benutzer die Zugriffsmodi Schreiben, Lesen, Ausführen unterscheidet,
  * Zugriffskontrollisten bis auf Einzelbenutzer.

Zusätzlich kann eine Retention-Period festgelegt werden:

- bei Jobvariablen für die Zugriffsmodi Schreiben, Lesen (ohne Zugriffskontrollisten).
- bei Bändern, durch Eigentümerschaft des Bandes und Ausschließlichkeitsanzeige (SHARE=NO) geregelt, die bei Übereinstimmung des Eigentümers der Datei und des Bandes durch das entsprechende Attribut der ersten Datei auf einem Band gesetzt werden. Über den Bandkatalog MARENCAT (Subsystem MAREN) kann ein Band zusätzlich geschützt werden: bei nicht mit SHARE=NO geschützten Bändern können eine effektive Eigentümerschaft und neue effektive Schutzattribute (kein Sharing mit anderen Benutzern oder nur Lesezugriff durch andere Benutzer) sowie ein Paßwort (wie für Dateien) und eine Retention-Period festgelegt werden.

Memory-Pools und Event-/Serialisations-Items sind den Taskprozessen zugeordnet, die sich an sie angeschlossen haben. Sie werden durch den ersten Taskprozeß erzeugt, wobei ihre Zugreifbarkeit festgelegt wird. Die Zugreifbarkeit wird durch den beim Erzeugen angegebenen Scope geregelt. Ein

Scope spezifiziert einen eigenen Namensraum, so daß er von allen Zugreifern in gleicher Weise spezifiziert werden muß.

Dabei bedeutet:

Scope = Local:	kein fremder Taskprozeß darf sich anschließen
Scope = Group:	alle Aufträge derselben Benutzerkennung dürfen sich (über Angabe des Namens) anschließen
Scope = User-Group:	alle Aufträge von Benutzerkennungen derselben Benutzergruppe dürfen sich anschließen
Scope = Global:	alle Aufträge dürfen sich anschließen

Auftragsbeschreibungen für Stapelaufträge oder Ausgabeaufträge sowie gestartete Stapelaufträge und Ausgabeaufträge sind jeweils einer Benutzerkennung zugeordnet und können nur von Aufträgen dieser Benutzerkennung modifiziert bzw. beeinflußt werden. Hier, ebenso wie bei exklusiv einem Taskprozeß zugeordneten Betriebsmitteln, erübrigt sich eine explizite Festlegung von Zugriffsrechten durch den Eigentümer.

Abprüfung von Zugriffen gegen Schutzattribute

Die Abprüfung von Zugriffen erfolgt für Dateien bei jeder Dateieröffnung (OPEN), für Jobvariablen bei jedem Zugriff, für Bänder beim Einspielen des Bandes und dem Open auf die erste Datei des Bandes.

Die Abprüfung des Zugriffs auf Memory-Pools und Event-/Serialisation-Items erfolgt über die Funktionseinheit NAME-MANAGER bei einem den eigentlichen Zugriffen vorgeschalteten Anmeldevorgang.

Ausnahmeregelungen

Die Eigentümerschaft einer Benutzerkennung an Dateien, Jobvariablen und Auftragsbeschreibungen gestarteter Aufträge kann vom Systemverwalter (Benutzerkennung TSOS) ersatzweise wahrgenommen werden (zur Abwehr von B.5). Ausgabeaufträge an einen RSO-Drucker haben als zusätzliche Ersatzeigentümer den Verwalter des RSO-Geräts, auf dem der Ausgabeauftrag ausgegeben werden soll.

Schutz der Information nach dem Löschen eines Objekts

Alle Adreßraumbereiche werden im BS2000-SC aufgrund der hier vorgeschriebenen Systemparametersetzung DESTLEV größer/gleich 4 vor der nächsten Zuweisung mit binären Nullen überschrieben.

Bei Jobvariablen ist immer nur der aktuell zugewiesene String auslesbar, so daß ein Löschen des Inhalts beim Löschen einer Jobvariablen entfallen kann.

Bei Bändern erfolgt ein Löschen des Inhalts nur durch Einrichten einer neuen leeren Datei mit dem Hinweis, nachfolgende Information zu löschen.

2.2 Sicherheitsfunktionalitäten

Dieses Kapitel stellt die Sicherheitsfunktionen nach Grundfunktionen geordnet dar.

Diejenigen Funktionalitäten, die über die Forderungen der Klasse F2 hinausgehen, sind durch Einrückung und eine kleinere Schrifttype kenntlich gemacht.

2.2.1 Identifikation und Authentisierung

Das System identifiziert und authentisiert Benutzer, die natürliche Personen sind, durch Prüfung einer vom Benutzer eingegebenen Benutzerkennung und des zugehörigen Paßworts oder der PIN beim Chip-Karten-Verfahren. Diese Identifikation erfolgt vor jeder anderen Interaktion des Systems mit

dem Benutzer. Nur nach einer erfolgreichen Identifikation und Authentisierung sind andere Interaktionen möglich. Nach der erfolgreichen Identifikation und Authentisierung wird die natürliche Person innerhalb des BS2000 durch Subjekte des BS2000 repräsentiert, die mit der Benutzerkennung gekennzeichnet sind.

Die Authentisierungsinformation ist im BS2000 in speziellen Dateien gespeichert, auf die - außer dem Authentisierungsmechanismus - nur explizit dazu autorisierte Benutzer über definierte Schnittstellen zugeifen können.

Bei jeder durchgeführten Interaktion kann das System die Identität des Benutzers aufgrund der Kennzeichnung der für ihn agierenden BS2000-Subjekte feststellen.

Bei nicht erfolgreicher Identifikation und Authentisierung des Benutzers wird der Rechnerzugang verweigert.

Neben der Identifikation und Authentisierung von Benutzern werden vom System auch Objekte, auf die der Benutzer bzw. Systemverwalter zugreifen kann, identifiziert.

Die Identifikation und Authentisierung der in der folgenden Liste aufgezählten Subjekte/Objekte stellt zum Teil eine zusätzliche, über die Grundforderungen der Funktionalitätsklasse F2 hinausgehende Funktionalität dar.

Identifizierte Objekte (in Klammern das Identifikationsmerkmal):

* *Ausgabe-und Benutzerauftrag (TSN oder JOB/SPOOLOUT-Name oder MONJV)*
* *Band-Datenträger (VSN)*
* *Benutzerkennung (relativ zu einem PVS durch CAT-ID und USER-ID)*
* *Benutzerschalter (relativ zu USER-ID über Numerierung)*
* *Bibliothekselement (relativ zu Bibliothek und Bibliothekstyp über Elementname und optionaler Versions- und Varianten-Angabe)*
* *Datei (Dateien sind durch die Katalogeinträge in Verbindung mit dem Dateiinhalt gegeben. Sie werden relativ zu CAT-ID bzw. CAT-ID, USER-ID oder LINK-Name identifiziert)*
* *Datei-ACL (ist einer Datei zugeordnet und wird daher relativ zu CAT-ID bzw. CAT-ID und USER-ID identifiziert)*
* *Datei-Linkeintrag (Name)*
* *DCAM-Anwendung (Name oder LINK-Name)*
* *Diskette (VSN)*
* *Event-/Serialisation-Item (relativ zu SCOPE)*
* *FITC-Connections (Port-Name)*
* *FITC-Ports (Port-Name)*
* *Geräte-Typen (Mnemonic)*
* *ITC-Items (globale Namen)*
* *Jobclass (Name)*
* *Jobvariable (relativ zu CAT-ID bzw. zu CAT-ID, USER-ID oder LINK-Name)*
* *Master-Catalog-Entry (Master-Catalog-Entries (MRS-Katalog-Einträge) sind jeweils einem PVS zugeordnet und werden durch die CAT-ID im MRSCAT identifiziert)*
* *Kommandosatz, eingeschränkte oder erweiterte Kommandomenge (Name der Gruppensyntaxdatei in Verbindung mit der Profile-Id). Innerhalb eines Kommandosatzes identifiziert das System Kommandos über Kommandonamen und den internen Namen. (Kommandoname, Standardname)*
* *Meldung (MSG-ID)*
* *Memory-Pool (relativ zu SCOPE)*
* *Page (Nr. relativ zum virtuellen Adreßraum)*
* *Programm (Programme sind als Bibliothekselemente in Bibliotheken od er als Dateien abgelegt. Sie werden durch ihren Ablageort, d.h. Bibliothek/Elementnamen oder Dateinamen identifiziert) (über Ablageort Datei bzw. Bibliothekselement oder Programmname)*
* *SPOOL-Gerät (Name)*
* *SPOOL-CHARACTER-SET (Name)*
* *SPOOL-Formular (Name)*
* *ARCHIVE-Sicherungsauftrag (ASN)*
* *TSOS-Sicherungsdatei (VSN, SVID und Dateiname ARCHIVE.SAVE.FILE; enthaltene Objekte durch Dateinamen bzw. Namen der Jobvariablen)*

* *Temporäre Datei, im Katalog speziell gekennzeichnet (relativ zu CAT-ID bzw. CAT-ID, USER-ID oder LINK-Name)*
* *Pubset (Cat-Id)*
* *Benutzergruppen (Name)*
* *Catalog (Kataloge in ihrer Gesamtheit stehen nur dem Systemverwalter zur Verfügung. Sie sind einem PVS zugeordnet und werden durch die CAT-ID im CMS identifiziert)*
* *Category (Name)*
* *Jobstream (Name)*
* *Shared-Program (Program-Name)*
* *Subsystem (Name, (optionale)Version)*
* *TSAP (Transport Service Access Point) (Prozessorname, Stationsname)*

Bei nicht erfolgreicher Identifikation von Subjekten/Objekten werden die entsprechenden Operationen mit Fehlermeldung (z.B. Returncode) abgewiesen. Die angestoßene Funktion wird nicht ausgeführt.

2.2.2 Rechteverwaltung

Benutzer werden nach ihrer erfolgreichen Identifikation und Authentisierung innerhalb des BS2000 durch eine Task repräsentiert (diese ist mit der Benutzerkennung gekennzeichnet), die im Auftrag des Benutzers arbeitet. **Die Objekte des BS2000, die der Rechteverwaltung im F2-Sinne unterliegen, sind im BS2000 die Dateien**. Die Dateien sind mit einer Datei-ACL (Access Control List) versehen, die für einzelne Benutzerkennungen/Benutzergruppen die Zugriffsrechte festlegt. Mögliche Datei-Zugriffsrechte sind Lesen, Schreiben und Ausführen. Mit Hilfe des ACL-Mechanismus ist es möglich, Benutzern bzw. Benutzergruppen den Zugriff auf eine ACL-geschützte Datei zu verwehren, den Zugriff auf einen nicht-modifizierenden Zugriff zu beschränken, sowie für jeden Benutzer separat die Zugriffsrechte an der Datei festzulegen.

Die Vergabe und der Entzug von Zugriffsrechten an einer Datei erfolgen durch den Eigentümer oder den Systemverwalter (TSOS) als Ersatzeigentümer. Damit ist die Weitergabe von Zugriffsrechten kontrollierbar.

Das Einbringen/Löschen/Sperren neuer Benutzer/Benutzergruppen ist nur möglich durch autorisierte Benutzer, die das Systemverwalterrecht USER-ADMINISTRATION bzw. das Gruppenverwalterrecht MANAGE-MEMBERS bzw. MANAGE-GROUPS haben. Ein automatisches Sperren nach Fehlversuchen erfolgt nicht.

Neben den Zugriffsrechten zwischen Benutzer/Benutzergruppen als Subjekten und Dateien als Objekten und den Zugangsberechtigungen zum System werden im BS2000 noch weitere Rechte verwaltet. Das folgende ist eine Aufstellung weiterer von BS2000 verwalteter Rechte, ihres Umfangs und des zur Rechteverwaltung Berechtigten.

* *Band-Datenträger, Eigentümerrecht (gegeben entweder durch ausschließlichen Eigentümer der ersten Datei auf dem Band und/oder durch Eintrag im MAREN-Katalog).*
  Umfang:
  - *Ändern von Bandattributen*

  Zur Rechteverwaltung Berechtigter: Eigentümer oder autorisierter Benutzer mit dem Privileg TAPE-ADMINISTRATION
* *Band-Datenträger, Zugriffsrecht*
  Umfang:
  - *Zugriffsmodus (Schreiben/Lesen) durch Zugreifer oder autorisierten Benutzer mit PrivilegTAPE-ADMINISTRATION*
  - *Zugriff durch Nicht-Eigentümer*
  - *Retention-Period*

  Zur Rechteverwaltung Berechtigter: Eigentümer
* *SPOOL-Gerät, Verwalterrecht*
  Umfang:
  - *Abbruch von Ausgabeaufträgen und Informieren über deren Status, die dieses Gerät betreffen*
  - *(nicht prüfrelevante) Verwaltungsfunktionen bzgl. dieses Geräts*

  Zur Rechteverwaltung Berechtigter: SPOOL-Geräteverwalter oder Systemverwalter
* *Benutzerkennung (Rechte im Sinne von Attributen und Privilegien)*

Umfang Attribute:
- *RESIDENT-PAGES, CSTMP-MACRO-ALLOWED, TEST-OPTIONS*

Umfang Privilegien:
- *SAT-EVALUATION, SECURE-OLTP, USER-ADMINISTRATION, PRIVILEGE-ADMINISTRATION, TSOS, TAPE-ADMINISTRATION, NET-ADMINISTRATION*

* *PUBSET (Nutzungsrecht als Eintrag im Joinfile des PVS)*
Umfang:
- *Sichtbarkeit von Dateien*
- *PUBLIC-SPACE-LIMIT, PUBLIC-SPACE-EXCESS*

Zur Rechteverwaltung Berechtigter: Vergabe/Entzug durch Gruppenverwalter (MANAGE-MEMBERS) oder Benutzer mit Systemverwalterrecht USER-ADMINISTRATION

* *Kommandosatz, Ausführen von Kommandos*
Umfang:
- *Nutzung einer speziell eingeschränkten oder erweiterten Menge von Kommandos*

Die übrigen für die Systemverwaltung reservierten Rechte sind fest an das Systemverwalterrecht TSOS (ersatzweise an den Operator) gebunden. Dies betrifft die Objekte:
- *DCAM-Anwendung (Verwendung von $-Namen)*
- *Katalog*
- *Kategorie*
- *MRSCAT-Eintrag*
- *Pubset*
- *Shared-Program*
- *Subsystem*

BS2000 kennt über die Funktionalität von F2 hinausgehend bereits Rollen (ab F4 gefordert). Die Rollen im einzelnen sind:
- *Die Rolle der Systemverwaltung*
- *Die Rolle der Systembedienung (Operating)*
- *Die Rolle der Hardware-Wartung (nur Benutzerkennung SERVICE)*

Dabei ist die Rolle der Systemverwaltung noch weiter in die folgenden Unterrollen aufgegliedert:
Vorgegebene Rollen:
- *Audit-Auswerter (standardmäßig Benutzerkennung SYSAUDIT)*
- *Benutzerverwalter (beliebige Benutzerkennungen soweit bzgl. Rollen vereinbar)*
- *Sicherheitsbeauftragter (nur Benutzerkennung SYSPRIV)*
- *TSOS-Berechtigter (nur Benutzerkennung TSOS)*

Die Rollen des Audit-Auswerters, des Sicherheitsbeauftragten und des TSOS-Berechtigten sind wechselseitig unvereinbar.

Durch den Sicherheitsbeauftragten definierbare Rollen (Die Definition dieser Rollen erfolgt, indem sie einer anderen Benutzerkennung als TSOS zugeteilt werden):
- *Netz-Verwalter*
- *Tape-Verwalter*

2.2.3 Rechteprüfung

Beim Eröffnen einer Datei durch einen Benutzer muß die gewünschte Zugriffsart angegeben werden. Die Berechtigung des Benutzers, auf die Datei gemäß der angegebenen Zugriffsart zuzugreifen, wird geprüft. Liegt die nötige Berechtigung nicht vor, wird der Eröffnungswunsch abgewiesen. Liegt die nötige Berechtigung vor, wird die Datei gemäß der Zugriffsart geöffnet. Bei den darauf folgenden Zugriffsoperationen werden nur die beim Eröffnen der Datei spezifizierten Zugriffsarten zugelassen und andere abgewiesen.

Neben den Zugriffsrechten zwischen Benutzer/Benutzergruppen als Subjekte und Dateien als Objekte und den Zugangsberechtigungen zum System werden im BS2000 noch weitere Rechte geprüft, die jedoch nicht ohne weiteres in das F2-Schema einzuordnen sind. Das folgende stellt eine Aufzählung weiterer vom BS2000 vorgenommener Rechteprüfungen dar:

* *Benutzerkennung: Beim Systemzugang über LOGON prüft JOBACC die Jobklassenangabe und ob die maximale Anzahl von Fehlversuchen nicht überschritten wurde. SRPMAU prüft die Gültigkeit der USER-ID, die Zugangsklasse und das Paßwort. Im Falle des Zugangs mittels Chipkarte wird Chipkarten-Id und TSAP geprüft. Beim Systemzugang über ENTER prüft JOBACC die Jobklassen-*

angabe. SRPMAU prüft die Gültigkeit der USER-ID, die Zugangsklasse und das Paßwort. Beim Einrichten, Löschen und Ändern von Attributen einer Benutzerkennung wird das Recht MANAGE-MEMBERS geprüft.

* *Benutzergruppe: Beim Einrichten und Löschen von Benutzergruppen prüft SRPMUG das Recht MANAGE-GROUPS. Beim Ändern oder Anzeigen von Attributen prüft SRPMUG das Recht MANAGE-MEMBERS oder das Recht MANAGE-RESOURCES.*
* *DCAM-Anwendung: In DCAM wird geprüft, daß $-Namen nur durch TSOS-Berechtigten verwendet werden.*
* *Benutzeraufträge: Beim Zugriff auf Aufträge prüft JMS und STATUS das Eigentümerrecht.*
* *Ausgabeaufträge: Beim Zugriff auf Aufträge prüft RSO, STATUS und SPOOL das Geräteverwalterrecht oder das Eigentümerrecht.*
* *Banddatenträger: Beim Ändern/Anzeigen von Band-Attributen wird von MAREN das Eigentümerrecht oder das MAREN-Verwalterrecht TAPE-AMINISTRATION geprüft. Beim Zugriff auf Band-Datenträger wird von MAREN und DMSCMDA das Zugriffsrecht geprüft.*
* *Systemverwalterrechte (Ein Systemverwalterecht ist streng genommen kein Objekt. Dahinter verbirgt sich der Zugriff auf das Objekt Benutzerkennung bzw. die für die Benutzerkennung hinterlegten Privilegien.)*
  - *Bei der Benutzerverwaltung wird von SRPMAU, SRPMUG und SRPMUSER das Recht USER-ADMINISTRATION geprüft, bevor ein entsprechendes Gruppenverwaltungsrecht (MANAGE-GROUPS/MEMBERS) geprüft wird. Bei SHOW-LOGON-PROTECTION und JOINFOA wird zusätzliche Information für Berechtigte geliefert.*
  - *Bei der Privilegienverwaltung bzw. Änderung der SAT-Protokollierungsparameter wird von SRPMPR bzw. SAT das Recht PRIVILEGE-ADMINISTRATION geprüft.*
  - *Bei einer Vielzahl von Kommandos und SVCs wird das Recht TSOS geprüft, teilweise nur bzgl. einzelner Operanden (Einzelheiten siehe Prüfliste).*
  - *Bei der Bandverwaltung wird von MAREN das Recht TAPE-ADMINISTRATION geprüft.*
  - *Bei der Netzverwaltung wird von BCAM und ADAM das Recht NET-ADMINISTRATION geprüft.*
  - *Bei der Auswertung der SAT-Protokolldaten wird von SAT das Recht SAT-EVALUATION geprüft.*
* *Bei der Verwaltung von SPOOL-Geräten wird das SPOOL-Geräteverwalterrecht geprüft.*
* *Benutzerrecht: Beim Laden residenter Programme prüft VMM anhand von RESIDENT-PAGES die Obergrenze der für den Benutzer erlaubten Zahl von residenten Seiten. Bei einem Erhöhungswunsch bzgl. Testprivilegien prüft JMS, ob dieser Wunsch mit Berechtigung der Benutzerkennung vereinbar ist.*
* *PUBSET-Nutzungsrecht: In DMSCMDA, OPENCLOS erfolgt eine Abprüfung, ob ein PUBSET prinzipiell sichtbar ist für den Aufrufer. Bei der Belegung von Plattenplatz (FILEALLO) wird anhand von PUBLIC-SPACE-LIMIT geprüft, ob die Obergrenze erreicht wurde. Bei Überschreitung wird geprüft, ob das Recht PUBLIC-SPACE-EXCESS vorhanden ist.*
* *Kommandosatz: Beim Ausführen von Kommandos erfolgt in SDF eine Abprüfung auf Zulässigkeit gegenüber der Gruppensyntaxdatei.*
* *Event-/Serialisations-Item: Beim Zugriff wird von TM/NAMEMGR geprüft, ob der Zugreifer im Scope des Event-/Serialisations-Items liegt.*
* *Memory-Pool: Beim Anschlußversuch an einen Memory-Pool wird von VMM, CMP und NAMEMGR geprüft, ob derjenige, der den Anschluß wünscht, im Scope des Memory-Pools liegt. Beim Versuch einer Attributsänderung (Schreibschutz, Freigabe durch nicht CSTMP-Berechtigten) erfolgt durch VMM/CMP eine Prüfung des CSTMP-Rechts.*
* *Temporäre Datei: Beim Zugriff oder Löschversuch wird von DMSCMDMA geprüft, ob es sic um die erzeugende Task handelt.*
* *ARCHIVE-Sicherungsauftrag: Beim Ansprechen von ARCHIVE-Sicherungsaufträgen in ARCHIVE-Anw. wird durch ARCHIVE sichergestellt, daß ein unpriv. Benutzer nur seine eigenen Sicherungsaufträge ansprechen kann.*
* *TSOS-Sicherungsdatei: Bei gewünschter Kenntnisnahme von und Zugriff auf Inhalt von Sicherungsdateien durch einen Benutzer sorgt ARCHIVE dafür, daß ein Benutzer nur Informationen über die eigenen Dateien und Jobvariablen in der Sicherungsdatei erhält.*

Die Ausnahmen von den oben aufgezählten Rechteprüfungen betreffen hauptsächlich in irgendeiner Weise privilegierte Benutzer (TSOS, SERVICE usw.), die an der sonstigen Rechteprüfung vorbei über besondere Rechte verfügen.

Im Einzelnen:

Das Eigentümerrecht kann ersatzweise durch den TSOS-Berechtigten ausgeübt werden für die Objekte:

- *Ausgabeauftrag,*
- *Benutzerauftrag,*
- *Datei.*

Das Eigentümerrecht kann ersatzweise durch den Bandverwalter (TAPE-ADMINISTRATION) ausgeübt werden für das Objekt:

- *Band-Datenträger.*

Das Zugriffsrecht auf Dateien kann ersatzweise implizit durch den Benutzerverwalter (USER-ADMINISTRATION) oder einen Gruppenverwalter (MANAGE-GROUPS/MEMBERS) ausgeübt werden beim Löschen einer Benutzerkennung (Ausnahme: Systemkennungen, die beim Start des Systems eingerichtet werden). Das Zugriffsrecht kann ersatzweise durch den TSOS-Berechtigten ausgeübt werden für die Objekte:

- *Datei,*
- *Dateiattribute im PUBSET-Katalog,*
- *ARCHIVE-Sicherungsauftrag,*
- *TSOS-Sicherungsdatei.*

Beim Informierdienst (Kdo: SHOW-FILE-ATTRIBUTES, SVC: 144, 160) ist die Ausgabe der Paßwörter anforderbar. Sie werden nur in der verschlüsselten Form ausgegeben.

Das Zugriffsrecht kann ersatzweise durch den Bandverwalter (TAPE-ADMINISTRATION) ausgeübt werden für das Objekt:

- *Band-Datenträger.*

Das SPOOL-Geräteverwalterrecht kann ersatzweise durch TSOS ausgeübt werden.

Das Zugriffsrecht kann ersatzweise durch die Benutzerkennung SERVICE ausgeübt werden für die Objekte:

- *Datei,*
- *Dateiattribute im PUBSET-Katalog (betrifft nur Lesen),*

*wenn die entsprechende Datei vom Eigentümer mit dem Attribut "SPECIAL" gekennzeichnet worden ist (Kdo: CREATE-FILE ... und MODIFY-FILE-ATTRIBUTES, SVC: 144, 157), und - im Falle von Schutz über Zugriffslisten zusätzlich der geforderte Zugriff dort für SERVICE erlaubt ist (Basic-ACL: *OTHERS, ACL: Eintrag als Einzelbenutzer oder über die Gruppenzugehörigkeit etc.).*

Das Attribut PUBSET-LIMIT ist für den TSOS-Berechtigten unwirksam.

2.2.4 Beweissicherung

Das System enthält Protokollierungskomponenten gemäß den Anforderungen der Klasse F2. Zusätzlich werden bei allen Protokollsätzen die Merkmale "zugehörige Gruppe, wenn Benutzer legal; Audit-Id, wenn (bei Chipkartennutzung) bekannt" aufgezeichnet.

Es werden fünf Protokollmedien unterschieden

1. SAT für Systemverwalter und Benutzer,
2. CONSLOG für Systembediener,
3. OMNIS-LOG für OMNIS-Benutzer (unter Benutzerkennung TSOS),
4. SKP-LOG für den SKP-Benutzer und SKP-Startup,
5. DADM-LOG für Netzverwalter Kommandos (unter Benutzerkennung NAC)

Für 2. bis 5. ist eine Vorauswahl der aufzuzeichnenden Sätze nicht möglich. Es werden alle Interaktionen von Systembedienern aufgezeichnet, wobei auch Meldungen, die an die Systembedienung gesandt worden sind, aber aktuell nicht ausgegeben worden sind, mit aufgezeichnet werden.

Für SAT sind mehrere Möglichkeiten gegeben, eine Vorauswahl der aufzuzeichnenden Sätze zu treffen. Verantwortlich ist der Sicherheitsbeauftragte. Die beiden Systemverwalterrollen "Sicherheitsbeauftragter" (Benutzerkennung SYSPRIV) und "Audit-Auswerter" (üblicherweise insbesondere die Benutzerkennung SYSAUDIT) können dabei nicht ausgenommen werden: Alle ihre Aktionen werden bezüglich aller SAT-relevanten Ereignisse aufgezeichnet. Im übrigen kann eine Vorauswahl folgende Kriterien berücksichtigen:

- U: auslösende Benutzerkennung,
- E: Ereignisname einschl. Ergebnis (Erfolg/Mißerfolg),
- F: falls Datei betroffen: vom Eigentümer spezifizierte Audit-Angabe.

Für die logische Verknüpfung der Kriterien sind zwei grundsätzliche Wahlmöglichkeiten gegeben (die der Sicherheitsbeauftragte auch im laufenden Betrieb ändern kann):

Satz wird geschrieben, wenn

U oder E oder F

erfüllt ist, oder Satz wird geschrieben, wenn

U oder (E und F)

erfüllt ist.

Implizit werden Sätze aus Redundanzgründen unterdrückt, die bei den übergeordneten Ereignissen Taskterminierung und Programmterminierung bzgl. CLOSE-Ereignissen auf Dateien und bei Diskonnektion von Memory-Pools anfallen.

Standardmäßig wird bei CONSLOG folgende Information immer mitprotokolliert:

- Zeitpunkt (Datum, Uhrzeit),
- TSN der auslösenden Task bei Ausgaben bzw. Name der ausgebenden Anwendung,
- Kennzeichnung des Bedienungsplatzes bei Eingaben.

Da für jedes erfolgreiche LOGON bei der Taskerzeugung eine Meldung in CONSLOG geschrieben wird, die die Zuordnung USER-ID zu TSN enthält, ist damit für Ausgaben die Rückverfolgung auch zur USER-ID möglich.

Standardmäßig wird bei SAT folgende Information immer mitprotokolliert:

- Zeitpunkt (Datum, Uhrzeit)
- Ereignis-Id
- Ergebnis (Erfolg/Mißerfolg)
- TSN
- User-Id (soweit definiert)
- Group-Id (soweit User-Id definiert)
- Audit-Id (soweit definiert: Voraussetzung ist Chipkartennutzung)

Die protokollierten Ereignisse im Einzelnen:

Authentisierung

Subjekt: Natürliche Person oder Anwendung

Protokolliertes Ereignis und spezifische Information:

CHECK USER

* eingegebene User-Id
* Aufruftyp
* Terminal
* Application

ENABLE DIALOG

* Auftragstyp
* Return-Code (falls Ergebnis = Mißerfolg)
* Terminal

* Application

Subjekt: Benutzerkennung

Protokolliertes Ereignis und spezifische Information:

CHECK USER

* eingegebene User-Id
* Aufruftyp
* Returncode (falls Ergebnis = Mißerfolg)

ENABLE BATCH

* Auftragstyp (nicht bei Fehlversuch)
* User-Id des zu erzeugenden Auftrags
* TSN des erzeugten Auftrags

INITIATION

* TSN des auslösenden Auftrags
* Spoolin-Zeit

Zugriff auf Objekte

Objekt: Datei (Eigentümerrecht)

Protokolliertes Ereignis und spezifische Information:

CREATE SECURITY ATTRIBUTES

* Dateiname
* DMS-Returncode (falls Ergebnis = Mißerfolg)
* Audit-Attribut der Datei

MODIFY SECURITY ATTRIBUTES

* Dateiname
* DMS-Returncode (falls Ergebnis = Mißerfolg)
* Audit-Attribut der Datei

RENAME FILE

* Dateiname (alt)
* Dateiname (neu)
* DMS-Returncode (falls Ergebnis = Mißerfolg)
* Audit-Attribut der Datei

EXPORT SECURITY ATTRIBUTES /
IMPORT SECURITY ATTRIBUTES

* Dateiname
* DMS-Returncode (falls Ergebnis = Mißerfolg)
* Audit-Attribut der Datei

RENAME BY ARCHIVE

* Dateiname (alt)
* Dateiname (neu)
* DMS-Returncode (falls Ergebnis = Mißerfolg)
* Audit-Attribut der Datei

DELETE SECURITY ATTRIBUTES

* Dateiname
* DMS-Returncode (falls Ergebnis = Mißerfolg)
* Audit-Attribute der Datei

DELETE DATA

* Dateiname
* DMS-Returncode (falls Ergebnis = Mißerfolg)
* Audit-Attribut der Datei

Objekt: Datei-ACL (Eigentümerrecht)

Protokolliertes Ereignis und spezifische Information:

CREATE FILE ACL / DELETE FILE ACL / ADD FILE ACL ENTRY /

MODIFY FILE ACL ENTRY / REMOVE FILE ACL ENTRY

* Dateiname

Objekt: Datei (Zugriffsrecht)

Protokolliertes Ereignis und spezifische Information:

CREATE DATA / READ DATA / MODIFY DATA /

OPEN EXEC / DELETE DATA

* Dateiname
* DMS-Returncode (falls Ergebnis = Mißerfolg)
* Open-Modus
* Audit-Attribut der Datei

(Event ist abhängig vom Open-Modus, wobei die Modi INOUT, UPDATE, SINOUT auf MODIFY DATA, OUTPUT und OUTIN auf CREATE DATA, INPUT, REVERSE auf READ DATA abgebildet werden)

CLOSE FILE

* Dateiname
* DMS-Returncode (falls Ergebnis = Mißerfolg)
* Audit-Attribut der Datei

Objekt: Benutzerrecht/CSTMP-MACRO-ALLOWED
Protokolliertes Ereignis und spezifische Information:
CSTMP CALL
** Memory-Pool-Name*
** Scope*
Objekt: Benutzerrecht/TEST-OPTION
Protokollierung in CONSLOG, falls Wert größer 1 geschaltet wird
Objekt: DCAM-Anwendung
Protokolliertes Ereignis und spezifische Information:
Y-OPEN / Y-CLOSE
** Applikationsname*
** Host-Name (falls verschieden vom Default)*
** Return-Code*
CONNECT
** Applikationsname*
** Partnername*
** Partnertyp*
** Partner-Host (falls nicht lokal)*

** Connection-Id (falls Erfolg)*
DISCONNECT
** Applikationsname*
** Partnername*
** Partner-Host (falls nicht lokal)*
** Connection-Id*
Objekt: Benutzerauftrag
Protokolliertes Ereignis und spezifische Information:
TASK TERMINATION
** Termination-Typ*
** Termination-Grund*
MODIFY JOB
** TSN*
** RERUN-neu*
** FLUSH-neu*
** REPEAT-neu*
CANCEL JOB
** TSN*
Objekt: Ausgabeauftrag
Protokolliertes Ereignis und spezifische Information:
PRINT
** TSN (des erzeugten Auftrags)*
** Dateiname (ggf. zuzüglich Elementname mit Version und Typ)*
** ggf. ERASE*
** DMS-Returncode*
PUNCH
** TSN*
** Dateiname (ggf. zuzüglich Elementname mit Version und Typ)*
** ggf. ERASE*
** DMS-Returncode*
CANCEL SPOOL JOB
** TSN*
Objekt: Banddatenträger (Eigentümerrecht)
Protokolliertes Ereignis und spezifische Information:
USER MODIFY ATTRIBUTES
** VSN*
** Userid des Eigentümers*
Objekt: Banddatenträger (Zugriff)
Protokolliertes Ereignis und spezifische Information:
VOLUME PROCESSING
** VSN*
** Eigentümer*
** Dateiname*
Objekt: SPOOL-Gerät (Verwalterrecht)
Protokolliertes Ereignis und spezifische Information:
SPOOL DEVICE ADD / SPOOL DEVICE MODIFY
** Device*
** Administrator Userid*
** TSAP des Administrators*
SPOOL DEVICE REMOVE
** Device*
Objekt: Programm
Protokolliertes Ereignis und spezifische Information:
PROGRAM LOAD
** Dateiname*
** Elementname*
** Elementversion*
** Elementtyp*

** Internal-Name*
** Internal-Version*
** Internal-Datum*
** Load-Unit-Name*
** Context-Name*
Objekt: PUBSET, Nutzungsrecht
Protokolliertes Ereignis und spezifische Information:
SHOW FILE
** Cat-Id*
** Datei-Name (ggf. mit Wildcard)*
** Paßwort-Ausgabe (Ja/Nein)*
** Audit-Attribut der Datei (falls keine Wildcardeingabe)*
Anm.: Alle übrigen Kommandos und SVCs, die dieses Recht voraussetzen, werden im Erfolgsfall bei den entsprechenden Dateioperationen aufgezeichnet.
Objekt: Event-Items
Protokolliertes Ereignis und spezifische Information:
ENABLE EVENT / DISABLE EVENT / ENABLE SERIALISAT / DISABLE SERIALISAT
** Name*
** Scope*
Objekt: Memory-Pool
Protokolliertes Ereignis und spezifische Information:
ENABLE MP
** Name*
** Scope*
** Short-Id*
** Speicherklasse*
** Privileg*
** Access Key (0, ..., E, F)*
** Returncode*
DISABLE MP / $CSTMP-READABLE
** Name*
** Scope*
RELEASE MP
** Name*
** Scope*
Events, die keinem Objekt direkt zuordbar sind:
PROGRAM UNLOAD
** Internal-Name*
** Load-Unit-Name*
** Context-Name*

Ausübung von Systemverwalterrechten

Bereich: USER-ADMINISTRATION

Protokolliertes Ereignis und spezifische Information:

siehe "Zugriff auf Objekt Benutzerkennung/Benutzergruppe"

Bereich: PRIVILEGE-ADMINISTRATION

Protokolliertes Ereignis und spezifische Information:

SET PRIVILEGE / RESET PRIVILEGE

* User-Id

* Pubset

* angegebenes Privileg

HOLD SAT

* (keine weitere Satzinformation)

RESUME SAT
* Dateiname
MODIFY PRESELECTION
* alle Parameter (ggf. mehrere Sätze)

Bereich: TSOS (Systemfunktionen)
Protokolliertes Ereignis und spezifische Information:

OPEN VOLUME
* VSN
* DMS-Returncode (falls Ergebnis = Mißerfolg)
* Allocationtyp (shared/exclusive)
CLOSE VOLUME
* VSN
* DMS-Returncode (falls Ergebnis = Mißerfolg)
CATALOG EXPORT / CATALOG IMPORT
* Cat-Id
MODIFY SDF PARAMETER
* Name des eingestellten Syntaxfiles
* Typ des eingestellten Syntaxfiles
SS CREATION / SS DELETION / SS HOLD / SS RESUME
* Subsystem-Name
* Subsystem-Version
SS ADD
* Subsystem-Katalog

Bereich: TSOS (Utilities)
Protokolliertes Ereignis und spezifische Information:

UPDATE
* VSN (Original)
* VSN (Kopie)
* Device
* Device-Typ
VOLUME RELEASE / ACQUIRE
* VSN
* Device
* Device-Typ
INIT PROTECTED VOLUME / INIT UNPROTECTED VOLUME
* VSN (alt)
* VSN (neu)
* Eigentümer
* Neuer Eigentümer (falls definiert)
* Device

* Device-Typ

DISK INIT

* VSN (alt)
* VSN (neu)
* Device-Typ
* Funktion (Init, Formatierung)

IOCF-INSTALLATION

* Level

Bereich: TAPE-ADMINISTRATION

Protokolliertes Ereignis und spezifische Information:

ADD VOLUMES

* VSN
* Eigentümer (falls definiert)

REMOVE VOLUMES

* VSN
* Eigentümer (falls definiert)

ADMIN MODIFY ATTRIBUTES

* VSN
* Eigentümer (vorher)
* Eigentümer (nachher)

SHOW VOLUME ATTRIBUTES

* VSN
* Eigentümer

MODIFY MAREN PAR / SHOW MAREN PAR

* (keine weitere Satzinformation)

Bereich: NET-ADMINISTRATION

Protokolliertes Ereignis und spezifische Information:

ADAM

* Device (mn)
* Device-Typ

Bereich: SAT-EVALUATION

Protokolliertes Ereignis und spezifische Information:

SAT CHANGE FILE

* Dateiname (Success-Fall)
* Primary-Allocation
* Secondary-Allocation
* Block-Size
* VSN
* Device-Type

Objekt: Benutzergruppe

Protokolliertes Ereignis und spezifische Information:

DEFINE GROUP / MODIFY GROUP / REMOVE GROUP

* Group-Id,
* Pubset,
* Group-Id der übergeordneten Gruppe
* User-Id des Gruppenverwalters

SHOW GROUP

* Group-Id,
* Pubset

Objekt: Benutzerkennung

Protokolliertes Ereignis und spezifische Information:

ADD USER / MODIFY USER / USER LOCK / USER UNLOCK /
REMOVE USER / MODIFY LOGON PROTECTION /
SET LOGON PROTECTION / MODIFY USER PROTECTION

* User-Id,
* Pubset

Zusätzlich wird im Header des nachfolgenden SAT-Files die Ursache für den letzten Wechsel (Kdo, DMS-Fehler etc.) vermerkt.

2.2.5 Wiederaufbereitung

Speicherobjekte (Dateien, Banddatenträger, Memory-Pool, Page, EAM-Datei, Jobvariable, Event/Serialisation-Item, FITC-Port) werden vor einer Wiederverwendung so aufbereitet, daß keine Rückschlüsse auf ihren früheren Inhalt möglich sind.

2.2.6 Fehlerüberbrückung

Bezüglich Fehlerüberbrückung stellt die Funktionalitätsklasse F2 der IT-Sicherheitskriterien keine Forderungen. BS2000 V10.0 bietet aber auch in diesem Bereich eine gewisse Funktionalität.

Die Aufgabe der Fehlerüberbrückung ist es, Auswirkungen von Fehlverhalten des Systems zu begrenzen und so einen möglichst verlustfreien Ablauf zu gewährleisten.

Speicherfehler

* *Erkennung: HW-intern*
* *Maßnahmen der Überbrückung: Keine extern sichtbaren, da intern aufgrund vorhandener Redundanzen korrigiert.*

Plattenfehler: Schreib-/Lesefehler, Fehler der Aussteuerung (für alle Platten, die nicht als Shared-Pubsets verwendet werden)

* *Erkennung: Fehlerrückmeldung an Kanal - nach Ein-/Ausgabeauftrag*
* *Maßnahmen der Überbrückung: Nutzung der DRV-Funktion (Schreiben/Lesen auf und von zwei Platten gleichen Typs, wobei alle Pfade hierzu ebenfalls von gleichem Typ sein müssen)*

- *Nutzung des fehlerfreien Resultats;*
- *Egalisierung in Fehlerfälle, (implizit; auch explizit anstoßbar)*
- *Egalisierung bei dynamischem Zuschalten.*

CPU-Ausfall (bei Mehrprozessoranlagen)

* *Erkennung: Zentralprozessor bleibt stehen, was über Zeitstempel erkannt wird, oder MER setzt Kalt-Zustand für Logische Maschine.*
* *Maßnahmen der Überbrückung: Übernahme des auf fehlerhafter CPU unterbrochenen Kontextes durch andere CPU (falls Mehrprozessorsystem) und Fortsetzung. Bei Inkonsistenzen wird unter Umständen die auf der betroffenen CPU laufende Task oder der Systemlauf beendet.*

2.2.7 Gewährleistung der Funktionalität

Bezüglich der Gewährleistung der Funktionalität stellt die Funktionalitätsklasse F2 der IT-Sicherheitskriterien keine Forderungen. BS2000 V10.0 bietet aber auch in diesem Bereich eine gewisse Funktionalität.

Auch bei Eintreten von hardware- oder softwarebedingten Fehlern oder Störungen von außen soll ein möglichst ungestörter Betrieb aufrechterhalten werden.

Systemfunktionen werden generell vor Benutzerfunktionen priorisiert. Die Priorisierung erfolgt einzeln pro Taskprozeß. Fehler führen, je nach Schweregrad, zum Abbruch

a) eines Benutzerprogramms (Fehler wird behoben durch Zurücksetzen eines Programmlaufs),
b) eines Taskprozesses des Benutzers (Fehler wird behoben durch Zurücksetzen eines Taskprozesses),
c) des Systemlaufs (Fehler wird behoben durch Zurücksetzen eines Systemlaufs, z.B. aller System-globalen Sperren).

3. Beschreibung der Evaluation mit Hinweisen auf kritische Bereiche

Bei der Evaluierung von BS2000-SC Version 10.0 handelte es sich um eine entwicklungsbegleitende Evaluierung, bei der (Weiter-)Entwicklung, Dokumenten-Erstellung und Prüfung parallel durchgeführt wurden. Inkonsistenzen und Schwachstellen des Produkts und der Dokumentation im Hinblick auf das Evaluationsziel F2/Q3 konnten somit während der (und durch die) Evaluierung ausgeräumt werden.

3.1 Qualität der Sicherheitsanforderungen

Die Sicherheitsanforderungen an das System insgesamt mit den geforderten Sicherheitsfunktionen und der Bezug zu den Bedrohungen werden in natürlicher Sprache dargestellt. Die Sicherheitsanforderungen sind konsistent und vollständig. Die geforderten Sicherheitsfunktionalitäten entsprechen dem angestrebten Evaluationsziel.

3.2 Qualität der Spezifikation

Für jede Funktionseinheit als Hauptgliederungseinheit des Systems wurde eine in natürlicher Sprache gehaltene Design-Dokumentation, weitere Dokumente, die den Zusammenhang zwischen den Funktionseinheiten bzw. ihren Schnittstellen darstellen, und alle Manuale vorgelegt. Diese Dokumente bilden in ihrer Gesamtheit die Spezifikation und erfüllen in Verbindung mit den Sicherheitsanforderungen und den Quellcodes der Komponenten die Anforderungen.

Die Designspezifikationen beschreiben ausreichend detailliert die Funktionalitäten der Funktionseinheiten und dabei insbesondere die Sicherheitsmechanismen.

Der Zusammenhang zwischen den Sicherheitsanforderungen und den Funktionseinheiten wird durch die sogenannte "Prüfliste Sicherheitseigenschaften" hergestellt, die für jede Sicherheitsanforderung im Detail die sie realisierende Funktionseinheit benennt. Der Zusammenhang der Funktionseinheiten untereinander wird durch einen "Strukturbaum" dokumentiert.

Die Designspezifikationen beschreiben die jeweilige Funktionseinheit als Ganzes, in einer nächsten Stufe die einzelnen (logischen) Funktionen der Funktionseinheit und in einer weiteren die Prozeduren, die die niedrigste Stufe des hierarchischen Aufbaus darstellen. Die Abbildung der einzelnen Hierarchiestufen aufeinander wird durch den Strukturbaum in Verbindung mit den Designspezifikationen geleistet.

Die Abbildung der Prozeduren einer Funktionseinheit auf die Module des Quellcodes erfolgt, bis auf einige nicht sicherheitsrelevante Ausnahmen, explizit in den Designspezifikationen. In Verbindung mit der "Prüfliste Sicherheitseigenschaften" ist dadurch die Abbildung der Sicherheitsanforderungen bis auf den Quellcode nachvollziehbar.

Die als Spezifikation vorgelegten Dokumente sind insgesamt formal konsistent.

Es sind keine Nebeneffekte vorhanden, durch die Sicherheitsfunktionen umgangen oder außer Kraft gesetzt werden können.

Durch stichprobenhafte Quellcode-Untersuchungen wurde die Erfüllung der Sicherheitsanforderungen bestätigt.

3.3 Qualität der verwendeten Mechanismen

Die Mechanismen und Algorithmen sind in den zur Spezifikation des Systems gehörenden Designspezifikationen in Verbindung mit den Quellcodes im Detail beschrieben.

Die Mechanismen decken in ihrer Gesamtheit alle Sicherheitsanforderungen ab und erreichen eine Bewertung von "stark". In einem begründeten Ausnahmefall wurde ein Mechanismus mit "mittelstark" bewertet.

3.3.1 Mechanismen zur Identifikation und Authentisierung

Das Betriebsystem BS2000 in der nach F2/Q3 bewerteten Konfiguration bietet dem Benutzer die Zugangsklassen Dialog- und Batchzugang. Das System ist in beiden Fällen durch den Zwang zur Identifikation und Authentisierung des Systembenutzers vor unberechtigtem Zugang geschützt. **Die Zugangsklasse REMOTE BATCH ist in der nach F2/Q3 bewerteten Konfiguration nicht zugelassen.**

Die Authentisierung ist im BS2000 durch einen Paßwortmechanismus realisiert. Darüber hinaus ist dem Anwender durch den zusätzlichen Einsatz des Softwareproduktes ASECO die Möglichkeit gegeben, auch Chipkarten zur Authentisierung zu nutzen. Beide Authentisierungsmechanismen können gleichzeitig genutzt werden.

Nach erfolgreicher Zugangsprüfung erzeugt das System einen Benutzerprozeß, einen sogenannten Task. Dieser ist durch das Identifikationsmerkmal Task Sequence Number (TSN) eindeutig gekennzeichnet. Der Task ist dem Benutzer hierdurch in eindeutiger Weise zugeordnet. Dieser Mechanismus gewährleistet, daß jede durch einen Benutzer veranlaßte Aktion diesem eindeutig zuweisbar ist.

3.3.1.1 Authentisierung mittels des Paßwortmechanismus

Der Benutzer wird beim Paßwort-Mechanismus anhand einer Benutzerkennung (USER-ID) identifiziert. Die Vergabe der Benutzerkennungen erfolgt durch die Benutzerverwaltung. Beim Dialog-Zugang weist der Benutzer seine Authentizität durch die Eingabe des korrekten Paßwortes (Authentisierung durch Wissen) nach. Paßwörter werden in den BS2000-Manualen als Kennwörter bezeichnet. In der F2/Q3-Konfiguration wird durch die vorgeschriebene Systemparametersetzung ENCRYPT=Y erzwungen, daß Paßwörter immer einwegverschlüsselt abgespeichert werden.

Über die Kommandos SET-LOGON-PROTECTION und MODIFY-LOGON-PROTECTION können ausschließlich priviligierte Benutzer mit den Rechten eines systemglobalen Benutzerverwalters (USER-ADMINISTRATION) oder eines Gruppenverwalters mit dem Gruppenverwalterrecht MANAGE-MEMBERS oder MANAGE-GROUPS (dieser nur für die ihm untergeordneten Benutzerkennungen) Vorgaben an die minimale Länge, die Komplexität sowie die Lebensdauer von Paßworten machen.

Durch diese Kommandos kann auch der Systemzugang eines Benutzers gezielt auf bestimmte Datensichtstationen beschränkt werden.

Wenn zur Benutzerverwaltung berechtigte Benutzer ungeprüft möglicherweise unbefugt manipulierte Kommandoprozeduren aufrufen, die die Kommandos SET-LOGON-PROTECTION oder MODIFY-LOGON-PROTECTION enthalten könnten, so sind nicht bemerkte Änderungen der Authentisie-

rungsdaten möglich. Im Sicherheitshandbuch für die Systemverwaltung wird auf diese Bedrohung hingewiesen.

Um Probierattacken auf Paßwörter zu begegnen, ist die maximal erlaubte Anzahl an Fehlversuchen bei der Paßwortprüfung begrenzt. Darüber hinaus wird jeder Fehlversuch mit einer Zeitstrafe belegt.

Nach Verbindungsaufnahme und Eingabe des LOGON-Kommandos unter Angabe der Benutzerkennung sowie der Abrechnungsnummer erfragt das System das Paßwort. Die Eingabe des Paßwortes erfolgt bei dieser Vorgehensweise dunkelgesteuert. Das LOGON-Kommando gestattet aber auch die direkte Eingabe des Paßwortes als nicht dunkelgesteuerten Kommando-Operanden des LOGON-Kommandos. Im Sicherheitshandbuch für den Benutzer wird durch einen Warnhinweis auf diesen Umstand hingewiesen.

Der Bedrohung durch Spoofing Programme, auch als LOGON-Fallen bezeichnet, wird im BS2000 durch organisatorisch technische Maßnahmen, im wesentlichen durch die Nutzung eines Fluchtsymbols, des sogenannten TUI-Indikators, begegnet. Die erforderlichen Maßnahmen sind im Sicherheitshandbuch für den Systemverwalter sowie dem Sicherheitshandbuch für den Benutzer beschrieben.

3.3.1.2 Authentisierung durch Chipkarte

Wird die Chipkarte zur Authentisierung genutzt, so ist neben dem Besitz der Chipkarte (Authentisierung durch Besitztum) die Kenntnis der Personal Identification Number (PIN) (Authentisierung durch Wissen) erforderlich.

Beim Systemzugang identifiziert das BS2000-System den Benutzer zunächst anhand seiner Benutzerkennung. Ist für diese Benutzerkennung der Chipkartenschutz festgelegt, so wird der Benutzer aufgefordert, seine Chipkarte in das Chipkarten-Terminal einzuführen. Der Benutzer authentisiert sich zunächst durch Eingabe der Personal Identification Number (PIN) am Chipkarten-Terminal gegenüber der Chipkarte. Hierzu leitet das Chipkarten-Terminal die PIN direkt an die Chipkarte weiter, wo sie mit der dort verschlüsselt gespeicherten Referenz-PIN verglichen wird. Bei drei Fehlversuchen in Folge wird die Chipkarte gesperrt. War die Authentisierung des Benutzers gegenüber der Chipkarte erfolgreich, so erfolgt die Authentisierung der Chipkarte durch ein kryptographisches Verfahren. Die Schlüssel und der Verschlüsselungsalgorithmus sind nicht im BS2000-System sondern in einem seperaten Rechner, dem zentralen Autorisierungs-Terminal (ZAT), gespeichert. Das ZAT ist ein PC mit dem Betriebssystem MS-DOS. Hierdurch bedingt, sind zum Schutz des ZAT besondere organisatorische Maßnahmen erforderlich.

Die Nutzung der Chipkarte gestattet es, mehrere Personen einer Benutzerkennung zuzuordnen. Die Identifikation der Benutzer erfolgt dann eindeutig anhand der Chipkarten-ID (CID). Im taskspezifischen SRPM-Kontrollblock wird das Feld AUDIT_ID mit der Chipkarten-Id (CID) versorgt. Hierdurch ist sichergestellt, daß jede Aktion eines Benutzers im System auf diesen auch eindeutig rückführbar und somit eine personenbezogene Beweissicherung möglich ist.

Chipkarten werden mit Hilfe eines Personalisierungsrechners mit der CID und dem Kartenspezifischen Schlüssel versehen. Im System sind, wie auch bei der Vergabe von Benutzerkennungen, keine Mechanismen implementiert, die eine mehrfache Vergabe einer Chipkarten-ID an verschiedene Personen ausschließen. Die Eindeutigkeit bei der Vergabe der Chipkarten-ID ist durch organisatorische Maßnahmen sicherzustellen.

Der Personalisierungsrechner wird getrennt vom BS2000-System betrieben.

3.3.2 Mechanismen zur Rechteverwaltung

3.3.2.1 ACL-Mechanismus zur Verwaltung der Dateizugriffsrechte

Im BS2000 sind die Dateien diejenigen Objekte, die der Rechteverwaltung im Sinne der Anforderungen der Funktionalitätsklasse F2 unterliegen.

Die Dateien werden in geschützten Systemdateien, den sogenannten Dateikatalogen, verwaltet. Hier werden sie durch Katalogeinträge, Catalog Entries, repräsentiert. Diese enthalten unter anderem den Dateinamen, die Benutzerkennung des Datei-Eigentümers sowie Dateiattribute. Der Zugriff auf einen gesuchten Katalogeintrag erfolgt über den Pfadnamen (Katalog-Id, User-Id, Dateiname). Die Katalogeinträge eines Benutzers sind in einer logischen Kette angeordnet, wobei jedem Benutzer seine Primary Block Number (PBN), die den ersten Katalogeintrag des Benutzers kennzeichnet, zugeordnet ist.

Die Anforderungen an die Rechteverwaltung nach F2 werden durch den ACL-Mechanismus realisiert.

Dieser ermöglicht es, die Dateizugriffsrechte für einzelne Benutzer und Benutzergruppen festzulegen. Als Dateizugriffsrechte können das Lese-, das Schreib- oder das Ausführungsrecht an dieser Datei vergeben werden.

Die Benutzerkennungen bzw. die Benutzergruppen, an die Zugriffsrechte zu einer durch den ACL-Mechanismus geschützten Datei vergeben wurden, sind neben den jeweils an sie vergebenen Zugriffsrechten in Datei-Zugriffskontrollisten, den Datei-ACL, eingetragen. Neben den benutzer- bzw. benutzergruppen-spezifischen Rechten können in der Datei-ACL auch sogenannte Default Access Rights (DAR) eingetragen werden. Diese Zugriffsrechte an der Datei gelten für alle Benutzer, deren Benutzerkennung oder Gruppenkennung nicht in der Datei-ACL eingetragen sind.

Der erweiterte Zugriffsschutz für Dateien über den ACL-Mechanismus ist explizit für eine Datei durch den Eigentümer der Datei durch das Erzeugen der Datei-ACL zu aktivieren. Nur der Eigentümer einer Datei und ersatzweise der Benutzer mit dem SystemverwalterRecht TSOS können die Zugriffsrechte in der Datei-ACL eintragen, modifizieren und löschen. Der Eigentümer der Datei kann auch sich selbst das Zugriffsrecht nehmen, es sich aber jederzeit als Eigentümer wieder geben.

Die Bezeichnung der Datei-ACLs ist eindeutig, da es keine Möglichkeit gibt, den Namen einer Datei-ACL mehrfach zu vergeben.

Alle Datei-ACL eines Pubsets sind ihrerseits in einer ACL-Datei abgelegt. Diese ist durch das System vor unberechtigtem Zugriff geschützt.

Die Zugriffsrechte zu Dateien können nur positiv vergeben werden. Ein Zugriffsverbot für bestimmte Benutzerkennungen ist dadurch zu realisieren, daß weder an die Benutzerkennung selbst, noch an deren Benutzergruppe, noch standardmäßig gültige Zugriffsrechte (DAR-Eintrag) vergeben werden.

3.3.2.2 Mechanismen zum Einbringen, Löschen und Sperren von Benutzern

Im BS2000 wird ab der Version 10.0 die Möglichkeit geboten, Benutzerkennungen zu Benutzergruppen zusammenzufassen. Die Benutzergruppen sind in einer hierarchischen Baumstruktur angeordnet. Die Wurzel der Gruppenstruktur bildet die bei First-Start auf dem Home-Pubset eingerichtete Gruppe *UNIVERSAL. Alle Benutzerkennungen, die nicht explizit durch ein Kommando einer definierten Gruppe zugeordnet worden sind, gehören der Wurzelgruppe *UNIVERSAL an.

Jede Benutzergruppe hat einen eindeutigen Namen und besitzt ein gruppenspezifisches Kontingent an Gruppenbetriebsmitteln und Rechten des Gruppenverwalters.

Das System kennt das systemglobale Benutzerverwalterrecht USER-ADMINISTRATION und das Gruppenverwalterrecht ADM-AUTHORITY in seinen hierarchisch geordneten Ausprägungen MA-

NAGE-RESSOURCES, MANAGE-MEMBERS, MANAGE-GROUPS. Das systemglobale Benutzerverwalterrecht ist den Gruppenverwalterrechten übergeordnet. Standardmäßig ist das Privileg USER-ADMINISTRATION an die Benutzerkennung TSOS vergeben. Der Sicherheitsbeauftragte mit der Benutzerkennung SYSPRIV kann dies Privileg an jede Benutzerkennung, sich selbst ausgeschlossen, vergeben.

Die Gruppenverwalterrechte sind im Einzelnen:

MANAGE-RESOURCES:

Der Gruppenverwalter ist berechtigt Betriebsmittel und Benutzerrechte der Benutzerkennungen, die seiner eigenen Gruppe oder der ihr untergeordneten Gruppenstruktur angehören, zu verwalten.

Er hat kein Recht, Benutzerkennungen anzulegen, zu löschen und von einer Benutzergruppe zur anderen zu transferieren.

Er hat kein Recht, die Organisation (Hierarchie) der Benutzergruppen zu ändern, d.h. er kann Benutzergruppen weder anlegen, noch transferieren oder löschen.

MANAGE-MEMBERS:

Der Gruppenverwalter ist berechtigt, Benutzerkennungen innerhalb seiner eigenen oder einer dieser untergeordneten Benutzergruppe neu anzulegen, zu modifizieren, zu löschen und zu deaktivieren.

Die MANAGE-MEMBERS-Berechtigung impliziert die MANAGE-RESOURCES-Berechtigung.

MANAGE-GROUPS:

Der Gruppenverwalter ist berechtigt, die Organisation der hierarchisch unter seiner Benutzergruppe liegenden Gruppen durch Neuanlage, Löschen und Transferieren von Benutzergruppen zu verändern.

Die MANAGE-GROUPS-Berechtigung impliziert das MANAGE-MEMBERS-Recht.

Jede Gruppe kann, muß aber nicht notwendigerweise einen Gruppenverwalter haben. Gruppenverwalter der Wurzelgruppe *UNIVERSAL sind alle Benutzerkennungen mit Privileg USER-ADMINISTRATION. Ein Gruppenverwalter wird entweder durch den Gruppenverwalter einer höheren Gruppe - sofern dies Recht in dessen Gruppenpotential enthalten ist - oder einem Benutzer mit dem Privileg USER-ADMINISTRATION ernannt. Gruppen können neben dem Gruppenverwalter auch jederzeit von einem Benutzer mit dem Privileg USER-ADMINISTRATION verwaltet werden.

3.3.3 Mechanismen zur Rechteprüfung beim Dateizugriff (ACL-Mechanismus)

Wurde für eine Datei der erweiterte Zugriffsschutz durch den ACL-Mechanismus aktiviert, so wird im Katalogeintrag dieser Datei ein entsprechendes Attribut gesetzt. Ist dies Attribut gesetzt, so stellt das System vor dem Öffnen der Datei sicher, daß die zugehörige Datei-ACL ausgewertet wird. Nur die als Ergebnis dieser Auswertung für den aufrufenden Benutzer als zulässig erkannten Zugriffsarten sind möglich.

Das sequentielle Lesen der ACL-Datei ist nur dem Benutzer mit dem Systemverwalterrecht TSOS möglich.

Wird eine Datei gelöscht, so wird auch ihre Datei-ACL gelöscht.

Wenn eine Benutzerkennung gelöscht oder neu vergeben wird oder aber eine Benutzergruppe verändert oder gelöscht wird, so wird dies bezüglich der Datei-ACLs nicht berücksichtigt. Dies bedeutet, daß hier organisatorisch Vorsorge zu treffen ist.

3.3.4 Mechanismen zur Beweissicherung

3.3.4.1. SAT-Mechanismus

Im BS2000 ist die Auswahl und die Aufzeichnung der Protokollinformationen zu Aktionen von Systemverwaltung und Benutzern durch eine zentrale Komponente (SAT) realisiert. Über eine standardisierte Schnittstelle wird diese Protokollierungskomponente von denjenigen Systemkomponenten aufgerufen, in denen zu protokollierende Ereignisse anfallen. Die zu protokollierenden Informationen erhält die Protokollierungskomponente über diese standardisierte Schnittstelle.

Die Nichtumgehbarkeit der Beweissicherung wird wesentlich durch diejenigen Systemkomponenten des BS2000 gewährleistet, die die Protokollierung durch den Aufruf von SAT anstoßen.

Bei der Bearbeitung eines Ereignisses entscheidet SAT anhand eigener Datenstrukturen und anhand SRPM -Informationen, ob und wie ein Ereignis zu protokollieren ist.

3.3.4.2. Zugriff zu den Protokollinformationen

Der Zugriff zu den Protokollinformationen ist nur autorisierten Benutzern möglich, da diese Informationen in Dateien abgelegt sind, die nicht autorisierten Benutzern nicht zugänglich sind. Die Dateien CONSLOG, SAT, SKP-LOG und SAVEREP sind unter der Benutzerkennung SYSAUDIT abgelegt. Die Datei OMNIS-LOG ist unter der Benutzerkennung TSOS abgelegt. Die Datei DADM-LOG ist unter der Benutzerkennung NAC abgelegt. Die Dateien werden systemseitig geschrieben, wobei die Auswahl der zu schreibenden Information für SAT von SYSPRIV gesteuert wird über die Einstellung von Vorselektionskriterien.

Der Zugriff auf diese Protokolldateien ist nur unter der Benutzerkennung SYSAUDIT möglich (Ausnahme TSOS), wobei der Zugriff für SYSAUDIT über geeignete Dienstprogramme eingeschalt ist.

Für SAT-Sätze ist eine besondere Engpaßbehandlung vorgesehen. Können Sätze nicht geschrieben werden, weil der Schreibpuffer gefüllt ist, wird der schreibende Taskprozeß angehalten. Nur Taskprozesse mit den Privilegien des Audit-Auswerters und des Sicherheitsbeauftragten können weiterhin Sätze schreiben (die dann im Adreßraum dieses Taskprozesses zwischengepuffert werden), um ihnen die Möglichkeit zu geben, den Dateiengpaß zu beseitigen. Ein Abbruch (LOGOFF, CANCEL) dieser Tasks ist vor Auflösung der Engpaßsituation nicht möglich.

3.3.4.3. Auswerte- und Verwaltungsprozeduren für die Protokolldaten

Es ist möglich, die Protokollierung auf einen oder mehrere beliebig wählbare Benutzer zu beschränken, wobei jedoch die Protokollierung von bestimmten Benutzern obligatorisch ist. Dies sind Benutzer mit besonders sicherheitskritischen Funktionen wie Sicherheitsbeauftragter, Audit-Auswerter und Operateure (d.h. Aktionen dieser Benutzer werden immer protokolliert). Wie weiter oben beschrieben: Die auslösende Benutzerkennung ist eines der Selektionskriterien dafür, ob ein Protokollsatz geschrieben wird oder nicht.

Zugriff und Auswertung auf die Protokolldateien CONSLOG, SAT, SKP-LOG und OMNIS-LOG ist über das Dienstprogramm SATUT eingeschalt.

Der Aufbau der Protokollsätze ist je nach Art des Protokolls verschieden, aber immer vollständig beschrieben. Dadurch, daß CONSLOG, SKP-LOG und OMNIS-LOG ein Mitschnitt von Interaktionen ist, ist der Aufbau dieser Protokollsätze teilweise durch die zugelassenen Kommando und Meldungsformate festgelegt.

3.3.5 Mechanismen zur Wiederaufbereitung

Speicherobjekte werden vor einer Wiederverwendung so aufbereitet, daß keine Rückschlüsse auf ihren früheren Inhalt möglich sind. Betroffene Speicherobjekte sind: Banddatenträger, Datei, Memory-Pool, Page, EAM-Datei, Jobvariable, Event/Serialisation-Item, FITC-Port.

Zeitpunkt der Wiederaufbereitung des Speichers:

* Banddatenträger: Einrichten einer Datei mit dem Attribut DESTROY-BY-DELETE auf Band
* Datei (Abhängig von Generierungsoption DESTLEV durch Eigentümer schaltbar): Löschen der Datei
* Memory-Pool: Anlegen des Memory-Pools
* Page: Anfordern der Seite
* EAM-Datei: Löschen einer EAM-Datei
* Jobvariable: Löschen einer Jobvariablen
* Event/Serialisation-Item: Bei Freigabe
* FITC-Port: Beim Einrichten eines Ports

3.4 Qualität der Abgrenzung zu nicht zu evaluierenden Systemteilen

Die Schnittstellen zu den zu evaluierenden Systemteilen und die entsprechenden Abgrenzungsmechanismen sind in den Sicherheitsanforderungen in Verbindung mit den relevanten Teilen der Spezifikation und der Manuale und weiteren speziellen Dokumenten beschrieben.

Die zu evaluierenden Systemteile sind diejenigen Systemteile, die nicht im unprivilegierten Prozessorzustand TU (Task Unprivileged) zum Ablauf gelangen. Zusätzlich zählen dazu einige ausgezeichnete Dienstprogramme. Die Schnittstellen im Sinne der Abgrenzung zu den nicht zu evaluierenden Systemteilen sind:

- Abgrenzung der systemintern genutzten Speicherseiten vor dem Zugriff durch unprivilegierte Benutzerprogramme
- Abgrenzung der Speicherseiten verschiedener Benutzerprozesse untereinander
- Kontrollierter Zugriff auf Systemdienste durch SVC-Aufrufe (Programmierschnittstelle)
- Kontrollierter Zugriff auf Systemdienste über Kommandos
- Schutz von systemseitig genutzten Daten bei der externen Speicherung durch Vergabe vorgeschriebener Schutzattribute (z.B. Dateipasswörter)
- Datenschnittstellen, d.h. vom Benutzer definierbare Dateien mit nicht trivialer Syntax des Inhalts, der vom System interpretiert wird (z.B. Lademodule)
- vom Benutzer initiierbare Unterbrechungen (Interrupts) im System.

Mit diesen Schnittstellen (bzw. den entsprechenden Schutzmechanismen) ist die Abgrenzung zu den nicht zu evaluierenden Systemteilen grundsätzlich gegeben. Anhand der Dokumentation ist nachvollziehbar, warum aufgrund der genannten Abgrenzungsmechanismen eine Beeinträchtigung oder Umgehung der Funktionen (insbesondere Sicherheitsfunktionen) der TCB (Trusted Computing Base = zu evaluierende Systemteile) nicht möglich ist. Die Aufgaben, Parameter und Effekte der Schnittstellen sind ausreichend dokumentiert.

Die Abgrenzungsfunktionen werden jeweils durch mehrere in der Regel voneinander unabhängige Einzelmechanismen realisiert, die einzeln und im Zusammenhang untersucht wurden und in ihrer Gesamtheit mit "stark" bewertet sind. Die Existenz der Mechanismen in der in den Dokumenten beschriebenen Form ist im Falle von Unklarheiten oder vermuteten Schwachstellen durch Tests und

durch stichprobenhafte Quellcodeuntersuchungen nachgewiesen. In einigen Fällen von Unklarheiten oder vermuteten Schwachstellen wurden anstelle von Tests Quellcodeuntersuchungen vorgenommen.

Abgrenzung des Systemadreßraums

Durch einen hardwaremäßig verankerten Schutzmechanismus (Schloß-Schlüssel-Mechanismus) wird gewährleistet, daß ein nicht privilegierter Benutzer nicht auf den Systemspeicherbereich zugreifen kann. Im Wartungsfall sind unter Anwendung von Autorisierungsmechanismen bestimmte Zugriffe auf den Systemspeicher möglich.

Abgrenzung der Taskadreßräume

Jeder Adreßraum bildet eine Domäne. Die Abschottung wird durch die Adreßumsetzung erreicht, die sich bei der Transformation einer virtuellen Adresse stets auf den eingeschalteten Adreßraum bezieht. Der einer Task zugeordnete Adreßraum wird bei der Initiierung der Task durch die Versorgung eines speziellen Hardware-Registers eingeschaltet. Alle folgenden Transformationsvorgänge beziehen sich damit nur auf den eingeschalteten Adreßraum.

Abgrenzung von Systemdiensten für SVCs

Die einzelnen Programmierschnittstellen werden durch gezielte Unterbrechungen des Programmlaufs eines Benutzerprogramms realisiert (Supervisor Calls SVCs). Nach der Analyse der im Aufruf spezifizierten Parameter und der Prüfung deren Legalität wird in den privilegierten Systemzustand gewechselt und die angeforderte Aktion ausgeführt.

Abgrenzung von Systemdiensten für Kommandos

Die Kommandos einschließlich aller Operanden werden über eine Eingabedatei vom SDF-Kommandoprozessor eingelesen. Vor der Ausführung der darin formulierten Anweisungen findet eine Syntaxprüfung statt, die sicherstellt, daß nur die vordefinierten Funktionalitäten des Systems vom Benutzer angestoßen werden können.

Abgrenzung von Systemdateien

Systemdateien liegen unter besonders geschützten Benutzerkennungen (z.B. TSOS). Sie sind über die Dateischutzmechanismen geschützt. Einige Systemdateien sind während des gesamten Systemlaufs geöffnet; auf sie kann nur über definierte Schnittstellen zugegriffen werden.

Datenschnittstellen

Eine dem Benutzer zugängliche und von ihm manipulierbare Datei (z.B. Lademodule) wird vom System im privilegierten Zustand geöffnet, gelesen und ausgewertet. Vor der Interpretation wird durch die Überprüfung des Inhalts der eingelesenen Daten sichergestellt, daß das Systemverhalten nicht durch gefälschte oder manipulierte Daten beeinflußt werden kann.

Unterbrechungen

Vom Benutzer initiierbare nicht über einen SVC-Interrupt abgewickelte Unterbrechungen sind

- programmbezogene Fehler
- programmbezogene Ereignisse
- Zeitgeberereignisse
- Rückmeldungen von E/A-Aufträgen

Diese Unterbrechungen entsprechen genau definierten Interrupts im System und lösen fest vorgegebene Aktionen des Systems aus, die nicht weiter beeinflußt werden können.

Schutz von Systemanwendungen

Das Transportsystem BCAM (Basic Communication Access Method) des Datenkommunikationssystems DCM (Data Communication Methods) muß bereitgestellt werden, da die Verbindung zwi-

schen Zentralprozessor, PDN-Vorrechnern, Konsolprozessoren und verschiedenen Verwaltungsinstanzen im Host in der Systemarchitektur als ein vernetztes System betrieben wird. Da BCAM beim Aufbau von angeforderten Verbindungen keine Privilegierungen kennt, hat jeder unprivilegierte Benutzer grundsätzlich Zugang zu BCAM und somit auch - über die vom System genutzten Zugänge zum BCAM-Netz - zu Komponenten des Systems. Diese Anwendungen sind vor nicht autorisiertem Zugriff durch unterschiedliche Mechanismen geschützt oder eine Adressierung wird erkannt und abgelehnt.

Die folgenden BCAM-Anwendungen dürfen im zertifizierten System **nicht** eingesetzt werden:

$ADS, $ATOP, $FJAM, $MRSAPP, $NDMS, $OBSERVE, $RBATCH.

3.5 Qualität des Herstellungsvorgangs

Die zur Implementierung des Systems verwendeten Sprachen weisen eine eindeutig definierte Syntax und gut dokumentierte Semantik auf.

Der Hersteller führte die Entwicklung des Systems in einem im "Methodenhandbuch" definierten und dokumentierten Gesamtprozeß durch. Die Verfahrensschritte "Entwicklung", "Integration/Qualitätssicherung" und "Auslieferung" erfolgen organisatorisch und personell getrennt. Somit ist insbesondere eine Rollentrennung zwischen Entwicklung und Testen der Software bei der Qualitätssicherung bzw. der Abnahme gegeben.

Die Herstellung der Software aus den Quellprogrammen ist durch das "Verfahren zur Herstellung der evaluierten Software aus den Quellprogrammen" dokumentiert. Die Übergabe der Quellprogramme von der Entwicklung an die Integration sowie die Übersetzung und das Zusammenbinden bei der Integration unterliegt einer Versions- und Änderungskontrolle. Diese ist im Methodenhandbuch beschrieben, wird durch das Produktions- und Leitsystem PULS EDV-unterstützt und meilensteinorientiert dokumentiert.

Das Software-Integrations- und Abnahmeverfahren wird im Methodenhandbuch beschrieben, dessen Einhaltung ist meilensteinorientiert dokumentiert.

Die vorgelegte Testbibliothek enthält neben den Testprogrammen alle Testergebnisse. Zusammen mit umfassenden Dokumenten - Spezifikationen der Tests, Testplan und Darlegung der Methoden - entspricht die Testbibliothek formal den Anforderungen.

Die auf der niedrigsten Hierarchiestufe der Spezifikation definierten Einheiten, die Prozeduren, sind als Module im Quellcode identifzierbar (cf. Kap. 4.2). Ihre Schnittstellen untereinander sind im Developers Handbook (DHB), in den entsprechenden Manualen, in den Prozedurbeschreibungen der Designdokumente und den Modulen des Quellcodes dokumentiert.

Tests - ergänzt durch Quellcodeanalysen und Nebenwirkungsanalysen - wurden zur Aufklärung von Unklarheiten und Schwachstellen durchgeführt. Unklarheiten und Schwachstellen konnten aufgeklärt bzw. behoben werden. Wege, durch die Sicherheitsfunktionen umgangen oder außer Kraft gesetzt werden können, wurden nicht gefunden.

Die Prüfung der Testbibliothek ergab, daß alle Systemteile durch Tests erfaßt werden. Durch eine eingehende inhaltliche Analyse ausgewählter Tests (zu SRPM, FACS, STATUS) ist nachgewiesen, daß die Testfälle im jeweiligen Kontext umfassend und plausibel sind und sicherheitsrelevante Aspekte ausreichend berücksichtigen. Diese Tests wurden nachvollzogen und lieferten die in der Dokumentation beschriebenen Ergebnisse.

Das vom Auftraggeber verwendete Verfahren zur Versions- und Änderungskontrolle wurde anhand einiger ausgewählter Programmodule, deren Weg von der Entwicklung bis zum tatsächlich ausgelieferten Datenträger nachvollzogen wurden, geprüft. Die Versionen (und Änderungen) der einzelnen

Komponenten sind in den Versionsständen erkennbar. Bei den geprüften Modulen bestehen keine Unstimmigkeiten zwischen dem vom Hersteller generierten und dem ausgelieferten System.

Die Unterlagen zur Software-Integration und -abnahme sind insgesamt vollständig. Die im Sinne einer Stichprobe untersuchte Übergabeerklärung zwischen der Qualitätssicherung und der Auslieferung, die im wesentlichen den erfolgreichen Abschluß der Testaktivitäten zum Ausdruck bringt, erwies sich im Abgleich mit den Planungsvorgaben als vollständig und konsistent.

3.6 Betriebsqualität

Unterschiedliche Möglichkeiten in der Konfiguration der Hardware sind im "Sicherheitshandbuch für die Systemverwaltung" dokumentiert (cf. Kap. 1.3.2). Sie haben keinen Einfluß auf die Sicherheitsanforderungen. Unterschiedliche Möglichkeiten der Konfiguration der Software sind nicht vorgesehen. Einige Subsysteme, die Sicherheitsfunktionen enthalten, sind jedoch insofern optional, als sie zwar generiert werden, aber nicht in jedem Fall gestartet werden müssen. Dies bedeutet aber keine Beeinträchtigung anderer Sicherheitsfunktionen. Diejenigen Subsysteme, auf deren Funktionalität nicht ohne Verlust der Sicherheit verzichtet werden kann, sind genau festgelegt (cf. Kap. 1.4). Sie sind im "Sicherheitshandbuch für die Systemverwaltung" entsprechend gekennzeichnet.

Der Prozeß der Generierung wird im Manual "Systeminstallation" und im "Sicherheitshandbuch für den Systemverwalter" beschrieben. Die Generierung wird von dem vielfältig einsetzbaren Werkzeug UGEN unterstützt und protokolliert. UGEN gehört als Produktionstool nicht zum zu evaluierenden Systemteil und wurde nur hinsichtlich der Protokollierung untersucht.

Bei der Systemgenerierung sind weitgehende, die spätere Wirksamkeit der Sicherheitsfunktionen des System beeinflussende Eingriffe bzw. Einflußnahmen möglich. Da verschiedene Tätigkeiten des Systemverwalters vom UGEN-Protokoll nicht erfaßt werden, ist eine lückenlose Beweissicherung im Sinne von Vollständigkeit, Korrektheit und Nachvollziehbarkeit durch administrative Maßnahmen sicherzustellen. Unter der Voraussetzung, daß die Auflagen korrekt und vollständig befolgt werden, sind keine nicht protokollierten Eingriffe möglich, die die Sicherheitsfunktionen außer Kraft setzen können. Die Generierung des Sytems ist anhand der Protokolle nachvollziehbar.

Die Übertragung der Software erfolgt mit Hilfe von Magnetbändern und nach dem Verfahren SOLIS. Durch einen Prüfbitmechanismus (Parity-Bits) werden Übertragungsfehler erkannt, die Übertragungsprozedur muß neu gestartet werden. Manipulationen des Masterbandes auf dem Weg zum Kunden werden durch Kuriertransport ausgeschlossen. **Die Erstinstallation erfolgt durch ein Team des Herstellers.** Durch diese Mechanismen bzw. Maßnahmen ist die Integrität der eingespielten Software sichergestellt.

Die Wartungssituation mit der damit verbundenen geringeren Systemsicherheit kann nur durch die Systemverwaltung oder durch autorisierte Benutzer herbeigeführt werden. Die Sicherheitsfunktionen des Systems gelten zumindest für den mit der Durchführung von Wartungsarbeiten beauftragten Benutzer und für die Dauer der Arbeiten als außer Kraft gesetzt. Wenn aufgrund des zur Wartung gewählten Zugangs eine Modifikation des Systems möglich war, gilt die Sicherheit des Systems bis zum nächsten Systemstart als nicht mehr gegeben. Das "Sicherheitshandbuch für die Systemverwaltung" weist auf die sicherheitsrelevanten Aspekte bei der Wartung hin und keine Inkonsistenzen auf.

Beim Einsatz von nicht evaluierten Korrekturen (REPs) gilt solange sich die Korrekturen im System befinden der Wartungsfall. Es darf nicht von der Wirksamkeit der Sicherheitsmechanismen ausgegangen werden.

Jede Wartung des PDN-Vorrechners zieht den Wartungsfall **dauerhaft** nach sich, d.h. der Zustand des Systems gilt nach einer Software-Wartung des PDN nicht mehr als zertifiziert.

Die beim Systemstart gegebenen Anweisungen und Parameter werden von den zur Ausführung gelangenden Systemkomponenten protokolliert. Nicht protokollierte Eingriffe, die die Sicherheits-

funktionen des Systems beeinflussen können, sind nicht möglich. Umgehungsmöglichkeiten der Protokollierung wurden nicht aufgedeckt.

Für die für das korrekte Funktionieren der Sicherheitsfunktionen wichtigen Hardware-Komponten (z.B. Hauptspeicher, Zentraleinheit, IO-Prozessoren) existieren Selbsttests. Die Selbsttesteinrichtung der Zentraleinheit wurde auf Vollständigkeit und Konsistenz der Dokumentation und Vollständigkeit und Plausibilität der Selbsttesteinrichtung an sich geprüft. Es wurden keine Mängel festgestellt.

3.7 Qualität der anwenderbezogenen Dokumentation

Die vom Hersteller ausgelieferten Dokumente beschreiben in ihrer Gesamtheit die durch die Sicherheitsanforderungen definierten Rollen und deren relevante Sicherheitsfunktionen, ihre Aufgaben und Benutzung. Sie stellen teils die sicherheitsrelevanten Schnittstellen zu Sicherheitsfunktionen, teils die Zusammenhänge zwischen verschiedenen Sicherheitsfunktionen und ggf. vorhandene Abhängigkeiten zwischen diesen dar.

Die Dokumentation ist vollständig, verständlich und handhabbar. Es gibt keine Abweichungen der benutzerbezogenen Dokumentation vom durch die Inspektion der Spezifikation oder durch Tests erkannten realen Systemverhalten.

Die Angaben zum Sicherheitsstatus der vom BS2000 unterstützten Geräte im "Sicherheitshandbuch für die Systemverwaltung" entsprechen stellenweise nicht den Vorgaben für den Betrieb des zertifizierten BS2000-SC V10.0. Die für den zertifizierten Betrieb zugelassenen Geräte sind den Tabellen in Kapitel 1.1.1 des vorliegenden Zertifizierungsberichtes zu entnehmen.

Nach dem Druck des "Sicherheitshandbuches für den Systemverwalter" wurden folgende Druckfehler entdeckt:

S. 435, Gerätetyp 3590: ersetze "+ 3590-B04/-B04" durch "+ 3590-B02/-B04"

S. 437: ersetze "9763-C Monochrom" durch "9763-C Colour"

S. 470, letzter Absatz, zweite Zeile: ersetze "systemglobaler Benutzerverwalter (USER-ADMINISTRATION)" durch "Systemverwalter (TSOS)".

4. Hinweise und Auflagen

Zur Installation und Generierung sowie zum Betrieb des BS2000-SC V10.0 sind die Vorgaben der in Kapitel 1.2 des Zertifizierungsberichtes aufgeführten Anwenderdokumente, insbesondere jene in den Sicherheitshandbüchern, unbedingt zu beachten.

Das zertifizierte Betriebssystem BS2000-SC V10.0 ist nur auf Sonderfreigabe erhältlich. Der Vertrieb erfolgt ausschließlich durch den Software-Kundendienst in München. Die Auslieferung der Software muß auf sicherem Vertriebsweg (Kuriertransport) erfolgen. Die Erstinstallation und Generierung des BS2000-SC V10.0 erfolgt durch Mitarbeiter des Herstellers. Die Systeminstallation und Generierung ist von mindestens zwei vertrauenswürdigen Personen (Vier-Augen-Prinzip) und ausschließlich auf dem rudimentären Rumpfbetriebssystem SIROS oder unter einem F2/Q3-System durchzuführen.

Bei der Systemgenerierung sind weitgehende, die spätere Wirksamkeit der Sicherheitsfunktionen des System beeinflussende Eingriffe bzw. Einflußnahmen möglich. Da verschiedene Tätigkeiten des Systemverwalters vom UGEN-Protokoll nicht erfaßt werden, ist eine lückenlose Beweissicherung im Sinne von Vollständigkeit, Korrektheit und Nachvollziehbarkeit durch die im Sicherheitshandbuch für die Systemverwaltung beschriebenen administrativen Maßnahmen sicherzustellen. Unter der Vor-

aussetzung, daß die Auflagen korrekt und vollständig befolgt werden, sind keine nicht protokollierten Eingriffe möglich, die die Sicherheitsfunktionen außer Kraft setzen können. Die Generierung des Sytems ist anhand der Protokolle nachvollziehbar.

Die Generierung der PDN-Phasen muß bei eingeschalteter Protokollierung (OPTION MSG=FH) erfolgen.

Der SKP muß so konfiguriert sein (Partnerprofil GENSKP, bzw. CSP), daß Konsolbetrieb nur von solchen Datensichtstationen aus möglich ist, die in sicherer Umgebung angeordnet sind. Der Konsolbetrieb darf weder über Teleservice möglich sein, noch darf Teleservice als Ersatzkonsole konfiguriert werden.

Der SKP muß so konfiguriert sein (Partnerprofil GENSKP, bzw. CSP), daß die Administration des SKP nur von den Konsolen aus möglich ist. Die Administration des SKP darf nicht von Teleservice aus möglich sein.

Die Protokollierung durch SKP-LOG ist für den Teleservice und für die Administration des SKP obligatorisch. Diese Protokollierung muß mit dem Schlüssel F (forced) eingestellt werden.

Für den Konsolbetrieb des BS2000 ist die Protokollierung zwar bereits durch CONSLOG abgedeckt, aber die Protokollierung des Konsolbetriebs durch SKP-LOG für den Zeitraum von Bedeutung, in dem das BS2000 nicht bzw. noch nicht läuft. Daher ist auch diese Protokollierung mit dem Schlüssel F (forced) einzustellen.

Die Zugangsklasse REMOTE BATCH ist in der nach F2/Q3 bewerteten Konfiguration nicht zugelassen.

Die folgenden BCAM-Anwendungen dürfen im zertifizierten System **nicht** eingesetzt werden:
$ADS, $ATOP, $FJAM, $MRSAPP, $NDMS, $OBSERVE, $RBATCH.

Nach First-Start und **vor dem Netzstart** muß die Paßwortvergabe an die Benutzerkennung TSOS erfolgen.

Das LOGON-Kommando gestattet auch die direkte Eingabe des Paßwortes als weiteren Operanden. Diese Form der Paßworteingabe ist nicht zulässig, da sie nicht dunkelgesteuert erfolgt.

Um der Ausspähung des eigenen Paßwortes durch Spoofing Programme, auch als LOGON-Fallen bezeichnet, zu begegnen, ist vor jedem LOGON durch die Eingabe des Umschaltindikators zusammen mit dem Kommando OPNCON eine neue Verbindung zwischen Datensichtstation und System aufzubauen.

Der lokale Wartungsmodus von Datensichtstationen ist durch Paßwort zu schützen.

Bei Benutzung der Chipkarte sind folgende organisatorische Maßnahmen erforderlich:

- Der Personalisierungsrechner muß vor dem Zugang durch Unbefugte geschützt sein, insbesondere gegen die Möglichkeit, Software unbefugt zu entnehmen oder einzubringen (z.B. Disketten).
- Unpersonalisierte Chipkarten müssen gegen Entwenden geschützt aufbewahrt werden.
- Personalisierte aber noch nicht vergebene Chipkarten müssen gegen Entwenden geschützt aufbewahrt werden.
- Der Betreiber des Personalisierungsrechners muß für die Eindeutigkeit der Personalisierung der Chipkarten sorgen, da die Funktionalität der Personalisierungssoftware dies nicht von sich aus garantiert.
- Das zentrale Autorisierungs-Terminal (ZAT) muß vor dem Zugang durch Unbefugte geschützt sein, insbesondere gegen die Möglichkeit, Software unbefugt zu entnehmen oder einzubringen (z.B. Disketten).
- Die Benutzer von Chipkarten müssen angehalten werden, selbst die nötige Sorgfalt zur Geheimhaltung ihrer PIN und gegen die Möglichkeit des Entwendens oder Verlierens der Karte walten zu lassen.

Beim Löschen von Benutzerkennungen bzw. von Benutzergruppen durch die Benutzerverwaltung werden die ACL-Einträge nicht automatisch aktualisiert. Das bedeutet, daß ACL-Einträge auch Namen von Benutzerkennungen und Benutzergruppen enthalten können, die im Betriebssystem nicht mehr existieren. Das BS2000 verhindert nicht, daß Benutzerkennungen und Benutzergruppen unter früherem Namen neu eingerichtet werden können, wenn der vorgesehene Name noch in einer Datei-ACL enthalten ist. Organisatorische Maßnahmen zur Vermeidung ungewollter Rechtebeziehungen beim Dateizugriff sind im SECOS-Manual beschrieben.

Im F2/Q3-System ist bei der Testprivilegierung für schreibende Speicherzugriffe maximal der Wert 3 zulässig. Solange ein Benutzer eine Testprivilegierung für lesende Speicherzugriffe mit einem Wert größer als 3 besitzt, gelten die Schutzmechanismen des Systems als außer Kraft gesetzt.

Sobald die Benutzerkennung $SERVICE aktiv ist, muß davon ausgegangen werden, daß der Wartungsfall vorliegt. Damit sind die Abgrenzungsmechanismen des Systems nicht mehr gewährleistet und ein F2/Q3-System ist nicht mehr gegeben.

Beim Einsatz von nicht evaluierten Korrekturen (REPs) gilt **dauerhaft** der Wartungsfall. Es darf dann nicht von der Wirksamkeit der Schutzmechanismen ausgegangen werden.

Nach einer Software-Wartung der PDN-Vorrechner befindet sich das System **dauerhaft** im Wartungsfall. Es darf dann nicht von der Wirksamkeit der Schutzmechanismen ausgegangen werden.